ExtremeXOS Installation and Release Notes

Software Version ExtremeXOS 12.0.2.25

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Published: November 2007
Part Number: 120361-00 Rev 14

AccessAdapt, Alpine, BlackDiamond, EPICenter, ESRP, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, the Go Purple Extreme Solution, ScreenPlay, Sentriant, ServiceWatch, Summit, SummitStack, Unified Access Architecture, Unified Access RF Manager, UniStack, UniStack Stacking, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodrive logo, the Summit logos, the Powered by ExtremeXOS logo, and the Color Purple, among others, are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

Adobe, Flash, and Macromedia are registered trademarks of Adobe Systems Incorporated in the U.S. and/or other countries. AutoCell is a trademark of AutoCell. Avaya is a trademark of Avaya, Inc. Merit is a registered trademark of Merit Network, Inc. Internet Explorer is a registered trademark of Microsoft Corporation. Mozilla Firefox is a registered trademark of the Mozilla Foundation. sFlow is a registered trademark of sFlow.org. Solaris and Java are trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2007 Extreme Networks, Inc. All Rights Reserved.

Contents

Chapter 1: Overview 5

New Features in ExtremeXOS 12.0.2 5
CLI Enhancements 5
Allowing Netlogin Egress Traffic 6
configure netlogin port allow egress 6
Description 6
Syntax 6
Forwarding with Disabled Learning Option 6
disable learning port 7
Description 7
Syntax Description 7
show ports information 7
Description 7
Syntax Description 7
Blackhole FDB Support 9
create fdbentry vlan ports 9
Description 9
Syntax Description 9
show fdb 10
show configuration 10
Multiport Unicast FDB Entries 11
create fdbentry vlan ports 12
L2 Edge License Supported Features 12
New Features in ExtremeXOS 12.0 15
New Hardware Supported in ExtremeXOS 12.0.2 17
Supported Hardware 17
BlackDiamond 10808 Switch Component Support 17
BlackDiamond 8800 Series of Switches Component Support 18
BlackDiamond 12800 Series Switches Component Support 19
Summit X150 Component Support 19
Summit X250e Component Support 20
Summit X450 Component Support 20
SFP (Mini-GBIC) Support 21
XENPAK Module Support 24
XFP Module Support 26
Summit X150 Series Switch Software Details 26
ExtremeXOS 12.0.2 (or later) Required 26
ExtremeXOS Command Line Support 27
Supported Commands on the Summit X150 Series Switches 27
Unsupported Commands on the Summit X150 Series Switches 40
Tested Third-Party Products 41
Tested RADIUS Servers 41
Tested Third-Party Clients 42
Legacy IP Phones 42
PoE Capable VoIP Phones 42

Extreme Switch Security Assessment 42
DoS Attack Assessment 42
ICMP Attack Assessment 42
Port Scan Assessment 43

Chapter 2: Upgrading to ExtremeXOS 12.0 45

Staying Current 45
Upgrading ExtremeXOS 45
Quick Summary 46
Detailed Steps 46
Upgrading ExtremeXOS on a Summit X150 51
Upgrading ExtremeXOS on a Summit X250e 52
Upgrading ExtremeXOS on a Summit X450 52
Upgrading an MSM-5 and MSM-5R to ExtremeXOS 12.0 on a BlackDiamond 12802 52
Upgrading a BlackDiamond Series of Switches Using Hitless Upgrade 54
Upgrading the Active Partition Using Hitless Upgrade 55
Upgrading the Alternate Partition Using Hitless Upgrade 56
Dual MSM Systems with Different Images Present 58
Using a Rev 10 (or later) BlackDiamond 10808 MSM-1 or MSM-1XL 58
Installing an ExtremeXOS Module 59
Uninstalling an SSH Module 60
Downgrading Switches 60

Chapter 3: Limits 63

Supported Limits 63

Chapter 4: Clarifications and Known Behaviors 77

Clarifications and Known Behaviors 77
Issues Resolved in ExtremeXOS 12.0.2.25 107
Issues Resolved in ExtremeXOS 12.0.2.18 107
Issues Resolved in ExtremeXOS 12.0.1.11 110

1 Overview

These Release Notes document ExtremeXOS™ 12.0. ExtremeXOS 12.0 enables new hardware products and software features.

This chapter contains the following sections:

- New Features in ExtremeXOS 12.0.2 on page 5
- CLI Enhancements on page 5
- L2 Edge License Supported Features on page 12
- New Features in ExtremeXOS 12.0 on page 15
- Supported Hardware on page 17
- Summit X150 Series Switch Software Details on page 26
- Tested Third-Party Products on page 41
- Extreme Switch Security Assessment on page 42

New Features in ExtremeXOS 12.0.2

Following are the new features supported in ExtremeXOS 12.0.2. These features will be documented in detail in the ExtremeXOS 12.1 versions of the *ExtremeXOS Concepts Guide* or the *ExtremeXOS Command Reference Guide*, unless otherwise noted.

CLI Enhancements

Following are the new software features supported in ExtremeXOS 12.0.2. These features are not documented in the *ExtremeXOS 12.0 Concepts Guide* or the *ExtremeXOS 12.0 Command Reference Guide*; however, they will appear in the soft revision of the guides.

- The option to allow broadcast and unicast traffic to egress an unauthenticated port.
- The option to forward any packets with unknown source MAC addresses has been added to the `disable learning port` command.
- The `blackhole` option has been added to the existing `create fdbentry` command for adding static FDB MAC forwarding entries.
- The ability to allow the addition of a multiport list to the creation of a static FDB unicast MAC forwarding entry using the `create fdbentry` command has been added.

See the appropriate following section for specific details:

- Allowing Netlogin Egress Traffic on page 6
- Forwarding with Disabled Learning Option on page 6
- Multiport Unicast FDB Entries on page 11

Allowing Netlogin Egress Traffic

This release introduces the ability to allow broadcast and unicast traffic to egress an unauthenticated port. You can allow a per port configuration of the egress traffic in unauthenticated state with the `configure netlogin port allow egress` command.

This command is available on all platforms.

NOTE

The `unicast` *and* `broadcast` *options are not available on the BlackDiamond® 10808 switch and the BlackDiamond 12800 series switches.*

configure netlogin port allow egress

```
configure netlogin ports [<port_list> | all] allow egress-traffic [none |
unicast | broadcast | all_cast]
```

Description

Configures the egress traffic in an unathenticated state.

Syntax

all	Specifies all netlogin ports.
port_list	Specifies one or more netlogin ports.
none	Specifies that no traffic is sent out if no authenticated clients exist on the VLAN.
unicast	Specifies that the unicast flooding traffic for the VLANs on the NetLogin enabled port be sent.
broadcast	Specifies that the broadcast traffic for the VLANs on the NetLogin enabled port be sent.
all_cast	Specifies that the broadcast and unicast flooding traffic for the VLANs on the NetLogin enabled port be sent.

Forwarding with Disabled Learning Option

This release introduces the ability to forward or drop packets with unknown source MAC addresses. You can disable MAC learning through selecting either `drop-packets` or `forward-packets` in the `disable learning port` command. MAC addresses learned on ports with learning enabled are manually programmed where at least one VLAN member exists to obtain the desired behavior.

This option is available only on the Summit® X450 switches.

This feature includes modifications in the `disable learning port` and `show ports information` commands. This section details the changes in the those commands, and supersedes the information in the *Extreme XOS 12.0 Command Reference Guide*.

disable learning port

```
disable learning {drop-packets | forward-packets} port [<port_list> | all]
```

Description

Disables MAC address learning on one or more ports for security purposes.

Syntax Description

port	Specifies the port.
port_list	Specifies one or more ports or slots and ports.
all	Specifies all ports and slots.
drop-packets	Specifies that packets with unknown source MAC addresses be dropped.
forward-packets	Specifies that packets with unknown source MAC addresses be forwarded.

show ports information

```
show ports {mgmt | <port_list>} information {detail}
```

Description

Displays detailed system-related information.

Syntax Description

mgmt	Specifies the management port.
port_list	Specifies one or more ports of slots and ports.
detail	Specifies detailed port information.

The output of the show ports information command has been modified so that when learning has been disabled with the `disabled learning port` command, a new "w" flag appears in the output. The following command displays port system-related information on a Summit X450a switch:

```
X450a-48t.10 # show port 1 info
```

Following is sample output from this command:

```
Port      Flags           Link          Link Num Num  Num   Jumbo QOS      Load
                          State     ELSM UPS  STP VLAN Proto Size  profile Master
=============================================================================
1         Ew------e--fMB- ready       -     0    0    1   1    9216  none
=============================================================================
> indicates Port Display Name truncated past 8 characters
Flags : a - Load Sharing Algorithm address-based, D - Port Disabled,
        e - Extreme Discovery Protocol Enabled, E - Port Enabled,
        g - Egress TOS Enabled, j - Jumbo Frame Enabled,
```

```
        l - Load Sharing Enabled, m - MACLearning Enabled,
        n - Ingress TOS Enabled, o - Dot1p Replacement Enabled,
        P - Software redundant port(Primary),
        R - Software redundant port(Redundant),
        q - Background QOS Monitoring Enabled,
        s - diffserv Replacement Enabled,
        v - Vman Enabled, f - Unicast Flooding Enabled,
        M - Multicast Flooding Enabled, B - Broadcast Flooding Enabled
        L - Extreme Link Status Monitoring Enabled
        w - MACLearning Disabled with Forwarding
```

The following command displays detailed port system-related information on a Summit X450a switch:

```
X450a-48t.11 # show port 1 info detail
```

Following is sample output from this command:

```
Port:   1
        Virtual-router: VR-Default
        Type:           UTP
        Random Early drop:      Unsupported
        Admin state:    Enabled with  auto-speed sensing  auto-duplex
        Link State:     Ready
        Link Counter: Up        0 time(s)


        VLAN cfg:
                Name: v1, Internal Tag = 4093, MAC-limit = No-limit, Virtual router:
VR-Default

        STP cfg:

        Protocol:
                Name: v1            Protocol: ANY      Match all protocols.
        Trunking:       Load sharing is not enabled.
        EDP:            Enabled
        ELSM:           Disabled
        Learning:       Disabled (forward-packets)
        Unicast Flooding:       Enabled
        Multicast Flooding:     Enabled
        Broadcast Flooding:     Enabled
        Jumbo:          Disabled
        Link up/down SNMP trap filter setting:  Enabled
        Egress Port Rate:       No-limit
        Broadcast Rate:         No-limit
        Multicast Rate:         No-limit
        Unknown Dest Mac Rate:  No-limit
        QoS Profile:    None configured
        Ingress Rate Shaping :          Unsupported
        Ingress IPTOS Examination:      Disabled
        Ingress 802.1p Examination:     Enabled
        Ingress 802.1p Inner Exam:      Disabled
        Egress IPTOS Replacement:       Disabled
        Egress 802.1p Replacement:      Disabled
        NetLogin:                       Disabled
        NetLogin port mode:             Port based VLANs
        Smart redundancy:               Enabled
        Software redundant port:        Disabled
```

```
        auto-polarity:                  Enabled
```

Blackhole FDB Support

This release adds support for the `blackhole` option to the existing `create fdbentry vlan ports` command. When the `blackhole` option is supplied to the command, any traffic received with a destination MAC address or source MAC address equal to the blackhole entry is dropped in hardware. When this happens, there is no software indication or notification.

This option is available only on the Summit X450 switches.

With existing releases of ExtremeXOS software, the `blackhole` option is only supported through access lists. For example, the following ACL policy would also blackhole traffic destined to or sourced from a specific MAC address:

```
entry blackhole_dest {
    if {
        ethernet-destination-address 00:00:00:00:00:01;
    } then {
        deny;
    }
}
entry blackhole_source {
    if {
        ethernet-source-address 00:00:00:00:00:01;
    } then {
        deny;
    }
}
```

A significant difference between the above ACL policy and the newly implemented `blackhole` option is the hardware used to implement the feature. Platforms with limited hardware ACL table sizes are able to implement this feature using the FDB table instead of an ACL table.

This feature includes the changes to the `create fdbentry vlan ports`, `show fdb`, and `show configuration` commands noted below.

create fdbentry vlan ports

```
create fdbentry <mac_addr> vlan <vlan_name> [ports <port_list> | blackhole]
```

Description

Creates a permanent static FDB entry.

Syntax Description

mac_addr	Specifies a device MAC address, using colon-separated bytes.
vlan_name	Specifies a VLAN name associated with a MAC address.

port_list	Specifies one or more ports or slots and ports associated with the MAC address.
blackhole	Enable the "blackhole" option; any packets with either source MAC address or destination MAC address matching the FDB entry are dropped

CLI <TAB> completion help text has also been added to help clarify the usage of the `blackhole` option. For example, if you enter the following command:

```
X450a-48t.12 # create fdbentry 00:01:02:01:02:01 "don" <TAB>
```

You see the following output:

```
blackhole       Drop packets with a destination MAC or source MAC matching this FDB
entry
```

show fdb

The show fdb command displays blackhole output under the `b` and `B` flags. The following command displays FDB information on a Summit X450a switch:

```
X450a-48t.12 # show fdb
```

Following is sample output from this command:

```
Mac                     Vlan       Age  Flags       Port / Virtual Port List
-------------------------------------------------------------------------------
00:00:00:11:22:33    Default(0001) 0000 spm  Bb

Flags : d - Dynamic, s - Static, p - Permanent, n - NetLogin, m - MAC, i - IP,
        x - IPX, l - lockdown MAC, L - lockdown-timeout MAC, M- Mirror, B - Egress
Blackhole,
        b - Ingress Blackhole, v - MAC-Based VLAN

Total: 1 Static: 1  Perm: 1  Dyn: 0  Dropped: 0  Locked: 0  Locked with Timeout: 0
FDB Aging time: 300
FDB VPLS Aging time: 300
```

show configuration

The `show configuration` command displays blackhole output. The following command displays configuration information on a Summit X450a switch:

```
X450a-48t.12 # show config fdb
```

Following is sample output from this command:

```
#
# Module fdb configuration.
#
create fdbentry 00:00:00:00:00:01 vlan "don" blackhole
```

Multiport Unicast FDB Entries

This release adds support for a feature that allows you to add a multiport list to the creation of a static FDB unicast MAC forwarding entry. This is also implemented using the `create fdbentry vlan ports` command. Currently, a multiport list is only allowed when the supplied MAC address is multicast. When a multiport list is supplied to the command, any traffic with a unicast destination MAC address equal to the FDB entry is multicasted to all ports in the list.

This option is available on the Summit X450a and Summit X450e switches.

You can use the `create fdbentry vlan ports` command to create a static FDB entry with a unicast MAC address and a list of more than one port. Once the static FDB is created, any ingress traffic with a destination MAC address matching the FDB entry is multicasted to each port in the specified list. On the Summit X450a and Summit X450e switches, if the FDB is the next hop for an IP adjacency, unicast routing sends the packet to the first port in the list.

However, the Summit X450a and Summit X450e switches do not support this feature natively using the FDB table. Instead, for each FDB entry of this type, a series of system ACLs have been installed which match the specified MAC address and VLAN ID, and override the egress port bitmap with the supplied list of ports. Multiple ACLs per FDB are required to handle Layer 2 echo kill by installing a unique ACL per individual port in the list to send matching traffic to all other ports in the list.

User-configured ACLs take precedence over these FDB-generated ACL rules. The hardware ACL limitations for these platforms are as follows:

- For "e series" platforms of the Summit X450 switches: 1K rules, 8 slices per group of 24 ports
- For "a series" platforms of the Summit X450 switches: 2K rules, 16 slices per group of 24 ports

The following command monitors the ACL rule resource:

```
X450a-48t.21 # show access-list usage acl-rule port 1
```

Following is sample output from this command:

```
Ports 1-24
Total Rules:      Used: 16  Available: 2032
```

The following command monitors the ACL slice resource:

```
X450a-48t.22 # show access-list usage acl-slice port 1
```

Following is sample output from this command:

```
Ports 1-24
Slices:           Used: 4  Available: 12
Slice 12 Rules:    Used: 5  Available: 123
Slice 13 Rules:    Used: 9  Available: 119
Slice 14 Rules:    Used: 1  Available: 127
Slice 15 Rules:    Used: 1  Available: 127
```

This feature includes the changes to the `create fdbentry vlan ports` command noted below.

create fdbentry vlan ports

The following command begins accepting unicast MAC addresses with multiple ports on all platforms except Summit X450a and X450e series platforms:

```
X450a-48t.13 # create fdbentry 00:00:00:00:00:01 "Default" port 1,2
```

Prior to this release, these platforms would report the following error:

```
Error: Does not support multiple port FDB entries for uni-cast MAC address!
```

The following command errors are still displayed to enforce the limitations on the Summit X450a switches:

```
X450a-48t.13 # create fdbentry 00:00:00:00:00:01 "Default" port 1:1,2:1
```

When the port list contains ports on different slots, the following error is generated:

```
Error: Multiple ports must be on the same slot for unicast MAC FDB entries.
```

L2 Edge License Supported Features

This release adds support for Summit X150 10/100 family of edge switches. This product family ships with the new "L2 Edge" license. The L2 Edge license includes all Layer-2 switch applicable capabilities of ExtremeXOS software that are not licensed by the higher license levels (the Edge, Advanced Edge, and Core licenses) or the Feature Packs. Table 1, Table 2, and Table 3 list the features included with these higher-level licenses. In cases where a feature is limited to specific platforms, that limitation is noted in the table.

NOTE

The L2 Edge license cannot be upgraded to a higher licensing level.

Table 1: ExtremeXOS Software Edge License Features

Feature	ExtremeXOS Software Version 12.0.2
Virtual L3 Switching (Virtual Routers), User Configurable	BlackDiamond 10808 Series BlackDiamond 12800 Series
Multinetting for Forwarding	All Platforms
Static IPv4 unicast routing	All Platforms
Static IPv6 unicast routing	All Platforms
Static IPv4 multicast routing	All Platforms
RIPv1/v2	All Platforms
RIPng	All Platforms
Routing Access Policies	All Platforms
Route Maps	All Platforms
Universal Port - VoIP Autoconfiguration	All Platforms
Universal Port - Dynamic user based security policies	All Platforms
Universal Port - Time of the Day policies	All Platforms

Feature	ExtremeXOS Software Version 12.0.2
Switch Stacking	Summit X450 Family Summit X250 Family

Table 2: ExtremeXOS Software Advanced Edge License Features

Feature	ExtremeXOS Software Version 12.0.2
VRRP	All Platforms
ESRP-Full	All Platforms
CLEAR-Flow	BlackDiamond 10808 Series BlackDiamond 12800 Series
OSPFv2-Edge (limited to max of 4 active interfaces)	All Platforms
PIM-SM-Edge (limited to max of 2 active interfaces)	All Platforms
MAC-in-MAC 802.1ah	BlackDiamond 10808 Series BlackDiamond 12800 Series
EAPS "Full" (multiple rings w/ multiple interconnect points)	All Platforms

Table 3: ExtremeXOS Software Core License Features

Feature	ExtremeXOS Software Version 12.0.2
EAPS "Full" (multiple rings w/ multiple interconnect points)	All Platforms
PIM DM "Full"	All Platforms
PIM SM "Full"	All Platforms
PIM SSM "Full"	All Platforms
OSPFv2 "Full" (not limited to 4 active interfaces)	All Platforms
OSPFv3 "Full" (not limited to 4 active interfaces)	All Platforms
BGP4	All Platforms
MSDP	All Platforms

For clarification, Table 4 provides a list of the L2 Edge license features available for the Summit X150 family of switches. Please note that this list is not complete.

Table 4: ExtremeXOS Software L2 Edge License Features

Feature	ExtremeXOS Software Version 12.0.2
EDP	All Platforms
LLDP 802.1ab	All Platforms
LLDP-MED extensions	All Platforms
VLANs – port based and tagged trunks	All Platforms
VLANS - mac based	All Platforms
VLANS - protocol based	All Platforms
VLAN Translation in VMANs	BlackDiamond 10808 Series BlackDiamond 12800 Series
VMAN Translation	BlackDiamond 10808 Series BlackDiamond 12800 Series
vMANs / Q-in-Q	All Platforms

Feature	ExtremeXOS Software Version 12.0.2
L2 Ping / Traceroute 802.1ag	BlackDiamond 10808 Series BlackDiamond 12800 Series
Jumbo Frames (including all related items, MTU disc. IP frag.)	All Platforms
QoS (all except rate shaping and hierarchical QoS)	All Platforms
QoS - rate shaping/limiting	All Platforms
Port trunking static 802.3ad	All Platforms
Port trunking dynamic (802.3ad LACP) Edge, to servers only	All Platforms
Port trunking dynamic (802.3ad LACP) Core, between switches	All Platforms
Port loopback detection and shutdown (ELRP CLI)	All Platforms
Software redundant port	All Platforms
STP 802.1D	All Platforms
STP EMISTP + PVST+ Compatibility Mode (1 domain per port)	All Platforms
STP EMISTP, PVST+ Full (multi-domain support)	All Platforms
STP 802.1s	All Platforms
STP 802.1w	All Platforms
ESRP aware	All Platforms
EAPS Edge (4 max domains with matching ring ports)	All Platforms
Link Fault Signaling (LFS)	All Platforms
ELSM (Extreme Link Status Monitoring)	All Platforms
ACLs	All Platforms
UDP BootP Relay Forwarding	All Platforms
Policy Based Routing	BlackDiamond 10808 Series BlackDiamond 12800 Series BlackDiamond 8800 a- and e-Series modules Summit X450 a- and e-Series switches
MSM Hitless Failover (for STP, ESRP)	BlackDiamond 10808 Series BlackDiamond 12800 Series BlackDiamond 8800 Series
MSM Hitless Failover - Additional capabilities: EAPS, NetLogin, PoE. Graceful Restart for OSPF, BGP	BlackDiamond 10808 Series BlackDiamond 12800 Series BlackDiamond 8800 Series
MSM Hitless Upgrade (for protocols supported by hitless failover)	BlackDiamond 10808 Series BlackDiamond 12800 Series
CPU DoS Protect	All Platforms
SNMPv3	All Platforms
SSH2 Server	All Platforms
SSH2 Client	All Platforms
SCP/SFTP Client	All Platforms
SCP/SFTP Server	All Platforms
RADIUS and TACACS+ per command authentication	All Platforms
Network Login - web-based method	All Platforms
Network Login - 802.1x method	All Platforms
Network Login - MAC based method	All Platforms

Feature	ExtremeXOS Software Version 12.0.2
Network Login - local database for MAC/Web based methods	All Platforms
Network Login - integration with Microsoft NAP	All Platforms
Network Login - multiple supplicants - same VLAN	All Platforms
Network Login - multiple supplicants - multiple VLANs	Summit X450 Family BlackDiamond 8800 Series
Network Login - HTTPS/SSL for web-based method	All Platforms
Trusted OUI	All Platforms
MAC Security - Lockdown	All Platforms
MAC Security - Limit	All Platforms
IP Security - DHCP Option 82	All Platforms
IP Security - DHCP Option 82 - VLAN ID	All Platforms
IP Security - Disable ARP learning	All Platforms
IP Security - DHCP IP Lockdown	All Platforms
IP Security - Gratuitous ARP Protection	All Platforms
IP Security - DHCP secured ARP/ARP Validation	All Platforms
IP Security - Trusted DHCP server ports	All Platforms
static IGMP membership, IGMP filters	All Platforms
IGMP v1/v2 Snooping	All Platforms
IGMP v3 Snooping	All Platforms
Multicast VLAN Registration (MVR)	All Platforms
sFlow accounting	All Platforms
CLI Scripting	All Platforms
Web-based device management	All Platforms
Web-based management - HTTPS/SSL support	All Platforms
XML APIs (for partner integration)	All Platforms
MIBs - Entity, for inventory	All Platforms

New Features in ExtremeXOS 12.0

Following are the new features supported in ExtremeXOS 12.0. These features are documented in detail in the *ExtremeXOS Concepts Guide* or the *ExtremeXOS Command Reference Guide,* unless otherwise noted.

- Stacking with hitless failover
- BlackDiamond 12802
- BlackDiamond 8800 10G4Ca I/O module
- Summit X250e series switch
  - Summit X250e-24P
  - Summit X250e-48P
  - Summit X250e-24T
  - Summit X250e-48T
- LX100 SFP optics support on all platforms

- 100FX SFP support on all BlackDiamond 8800 series and Summit X450 series switches
- Network Login
  - Precedence between local and RADIUS methods
  - Multiple supplicant multiple VLAN (BlackDiamond 12802 and BlackDiamond 12804 only)
- Protocol Anomaly Detection
  - Summit X450a and X450e series switch
  - BlackDiamond 8800 series switch with G48Te, G48Pe, G48Ta, G48Xa, 10G4Xa, 10G4Ca
- Policy-based redirect to port (L2 switched)
- Multicast Source Discovery Protocol (MSDP)
- IP route optimization
- OSPF Edge: scaling to four active interfaces
- VRRP VR awareness
- ESRP-aware selective forwarding
- vMAN enhanced feature set
  - STAG ethertype translation
  - SVID 1:N mapping
  - Inter vMAN traffic
  - Dynamic rate limiting configuration
- Fastpath IPv6 tunneling
  - Summit X450a and X450e series switch
  - BlackDiamond 8800 series switch with G48Te, G48Pe, G48Ta, G48Xa, 10G4Xa, 10G4Ca
- Mirroring in routed environment
  - Summit X450a and X450e series switch
  - BlackDiamond 8800 series switch with G48Te, G48Pe, G48Ta, G48Xa, 10G4Xa, 10G4Ca
- One-to-many mirroring
- QoS monitor statistics for BlackDiamond 8800 series and Summit X450 series switches
- Diffserv examination for vMAN traffic for BlackDiamond 8800 series and Summit X450 series switches
- Diffserv to vMAN dot1p mapping for BlackDiamond 8800 series and Summit X450 series switches
- Web-based device management (ScreenPlay)
- ExtremeXOS MIB parity with ExtremeWare:
  - extremeFdbMacFdbTable
  - extremeFdbIpFdbTable
  - IP forwarding MIB
  - Ping/traceroute MIB
- IPv6 mask change/hide CLI
- WAN PHY OAM BlackDiamond 12802 and BlackDiamond 12804 series switches
- Directed broadcast
- Custom web-based Network Login page
- SSH user-key based authentication
- SFTP support for downloading images

- SNMP trap filter for port up/down events
- VLAN statistics on a port
- Default initialization mode on a BlackDiamond 10808 or BlackDiamond 12804 only (ports come up as disabled and are not added to a default VLAN)

New Hardware Supported in ExtremeXOS 12.0.2

- Summit X250e series
  - Summit X250e-24x
- Summit X150 series
  - Summit X150-48t
  - Summit X150-24t
  - Summit X150-24p
- Optics
  - ER XFP
  - 10/100/1000 BASE-T Copper SFP
  - 100BASE-LX10 SFP
  - 100BASE-BX SFP
  - 100BASE-FX SFP (FE ports only)

Supported Hardware

Refer to the Extreme Networks hardware installation guides for more information about supported hardware. The following tables list the software filenames for the hardware that requires software.

BlackDiamond 10808 Switch Component Support

BlackDiamond 10808 components supported with ExtremeXOS 12.0, and the minimum ExtremeXOS version required by the chassis to support each component, include:

Table 5: BlackDiamond 10808 Component Support

BlackDiamond Component	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-1	bd10k-12.0.2.25.xos	10.1.0	1.0.1.5
MSM-1XL	bd10k-12.0.2.25.xos	10.1.0	1.0.1.5
10G2X	N/A	11.1.1	1.3.0.0
10G2H	N/A	11.2.0	1.3.0.0
10G6X	N/A	10.1.0	1.3.0.0
G20X	N/A	11.1.1	1.3.0.0
G60X	N/A	10.1.0	1.3.0.0
G60T	N/A	10.1.0	1.3.0.0
PSU Controller	N/A	1.0.1.0	N/A

Table 5: BlackDiamond 10808 Component Support (Continued)

BlackDiamond Component	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	10.1.0	N/A
1200 W DC PSU (Model # 60021/PS 2350)	N/A	1.0.1.0	N/A

BlackDiamond 8800 Series of Switches Component Support

BlackDiamond 8810 and BlackDiamond 8806 components supported with ExtremeXOS 12.0, and the minimum BootROM version required by the chassis to support each component, include:

Table 6: BlackDiamond 8800 Series of Switches Component Support

BlackDiamond 8810 and BlackDiamond 8806 Components	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-G8X	bd8800-12.0.2.25.xos	11.1.1.9	1.0.1.7
G48Te	N/A	11.5.1.4	1.0.1.10
G48Pe	N/A	11.5.1.4	1.0.1.10
G48Ta	N/A	11.5.1.4	1.0.1.10
G48Xa	N/A	11.5.1.4	1.0.1.10
G48P	N/A	11.1.1.9	1.0.1.7
G48T	N/A	11.1.1.9	1.0.1.7
G24X	N/A	11.1.1.9	1.0.1.7
10G4X	N/A	11.1.1.9	1.0.1.7
10G4Xa	N/A	11.6.1.9	1.0.1.11
10G4Ca	N/A	12.0.1.11	1.0.1.11
PSU Controller	N/A	11.1.1.9	2.13
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	11.1.1.9	N/A
600/900 W AC PSU (Model # 41050/PS 2431) (BlackDiamond 8806 only)	N/A	11.6.1.9	N/A
1200 W DC PSU (Model # 60021/PS 2350)	N/A	11.3.2.6	N/A
MSM-48	bd8800-12.0.2.25.xos	11.6.1.9	1.0.1.11

NOTE

Upgrading the BootROM on a BlackDiamond 8810 or BlackDiamond 8806 switch is not automatic when you upgrade the software. You must be running the minimum required BootROM version or later. Use the install firmware command after upgrading the ExtremeXOS image to insure the BootROM is at the latest level.

BlackDiamond 12800 Series Switches Component Support

BlackDiamond 12802, BlackDiamond 12804, BlackDiamond 12802 R-Series, and BlackDiamond 12804 R-Series components supported with ExtremeXOS 12.0, and the minimum BootROM version required by the chassis to support each component, include:

Table 7: BlackDiamond 12800 Series Switches Component Support

BlackDiamond 12802/12804 Components	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-5R (BlackDiamond 12804)	bd12k-12.0.2.25.xos	11.4.1.4	1.0.0.2
MSM-5R (BlackDiamond 12802)	bd12K-12.0.2.25.xos	12.0.1.11	1.0.0.2
GM-20XTR	bd12k-12.0.2.25.xos	11.4.1.4	N/A
XM-2XR	bd12k-12.0.2.25.xos	11.4.1.4	N/A
XM-2HR	bd12k-12.0.2.25.xos	12.0.2.25	N/A
MSM-5 (BlackDiamond 12804)	bd12k-12.0.2.25.xos	11.4.1.4	1.0.0.2
MSM-5 (BlackDiamond 12802)	bd12k-12.0.2.25.xos	12.0.1.11	1.0.0.2
MSM-6R	bd12k-12.0.2.25.xos	12.0.2.25	1.0.1.9
GM-20XT	bd12k-12.0.2.25.xos	11.4.1.4	N/A
GM-20T	bd12k-12.0.2.25.xos	11.4.1.4	N/A
PSU Controller	N/A	11.1.1.9	2.13
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	11.4.1.4	N/A
1200 W DC PSU (Model # 60021/PS 2350)	N/A	11.4.1.4	N/A

Summit X150 Component Support

Summit X150 series components supported with ExtremeXOS 12.0, and the minimum BootROM version required by the chassis to support each component, include:

Table 8: Summit X150 Component Support

Summit X150 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X150-24t	summitX-12.0.2.25.xos	12.0.2.18	1.0.3.1
Summit X150-48t	summitX-12.0.2.25.xos	12.0.2.18	1.0.3.1
Summit X150-24p	summitX-12.0.2.25.xos	12.0.2.18	1.0.3.1

Summit X250e Component Support

Summit X250e components supported with ExtremeXOS 12.0, and the minimum BootROM version required by the chassis to support each component, include:

Table 9: Summit X250e Component Support

Summit X250 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X250e-24p	summitX-12.0.2.25.xos	12.0.1.11	1.0.3.0
Summit X250e-48p	summitX-12.0.2.25.xos	12.0.1.11	1.0.3.0
Summit X250e-24t	summitX-12.0.2.25.xos	12.0.1.11	1.0.3.0
Summit X250e-48t	summitX-12.0.2.25.xos	12.0.1.11	1.0.3.0
Summit X250e-24x	summitX-12.0.2.25.xos	12.0.2.18	1.0.3.1

Summit X450 Component Support

Summit X450 components supported with ExtremeXOS 12.0, and the minimum BootROM version required by the chassis to support each component, include:

Table 10: Summit X450 Component Support

Summit X450 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X450a Series			
Summit X450a-48t	summitX-12.0.2.25.xos	11.5.1.4	1.0.2.2
Summit X450a-48tDC	summitX-12.0.2.25.xos	11.6.1.9	1.0.2.2
Summit X450a-24t	summitX-12.0.2.25.xos	11.5.1.4	1.0.2.2
Summit X450a-24tDC	summitX-12.0.2.25.xos	11.5.1.4	1.0.2.2
Summit X450a-24xDC	summitX-12.0.2.25.xos	11.6.1.9	1.0.2.2
Summit X450a-24x	summitX-12.0.2.25.xos	11.6.1.9	1.0.2.2
Summit X450e Series			
Summit X450e-24p	summitX-12.0.2.25.xos	11.5.1.4	1.0.2.2
Summit X450e-48p	summitX-12.0.2.25.xos	11.6.1.9	1.0.2.2
Summit X450 Series			
Summit X450-24x	summitX-12.0.2.25.xos	11.2.2.4	1.0.0.9
Summit X450-24t	summitX-12.0.2.25.xos	11.2.2.4	1.0.0.9
Option Cards			
XGM-2xn	summitX-12.0.2.25.xos	N/A	N/A
XGM2-2xn	summitX-12.0.2.25.xos	11.5.1.4	
XGM2-2xf	summitX-12.0.2.25.xos	11.5.1.4	

NOTE

Upgrading the BootROM on a Summit X450 switch is not automatic when you upgrade the software. You must be running the minimum required BootROM version. Use the `download bootrom` *command to download a BootROM image.*

SFP (Mini-GBIC) Support

SFPs supported on the BlackDiamond 8810 and BlackDiamond 8806 switches with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 11: BlackDiamond 8800 Series of Switches SFP Support

SFP	ExtremeXOS Required
1000BASE-T SFP	11.1.1.9
SX SFP	11.1.1.9
LX SFP	11.1.1.9
ZX SFP	11.1.1.9
100FX/1000LX SFP	11.3.1.3
100FX SFP	11.4.3.4 or 11.5.2.8 (not supported in 11.5.1.4)
1000BX SFP	11.4.1.4
LX100 SFP	12.0.1.11
10/100/1000BASE-T Copper SFP	12.0.2.18

SFPs supported on the BlackDiamond 10808 switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include

Table 12: BlackDiamond 10808 Switch SFP Support

SFP	ExtremeXOS Required
LX100 SFP	12.0.1.11
SX SFP	10.1.0
LX SFP	10.1.0
ZX SFP	10.1.0
1000BASE-T SFP	11.1.1.9
1000BX SFP	11.6.1.9

SFPs supported on the BlackDiamond 12804 switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 13: BlackDiamond 12804 Switch SFP Support

SFP	ExtremeXOS Required
SX SFP	11.4.1.4
LX SFP	11.4.1.4
ZX SFP	11.4.1.4
1000BASE-T SFP	11.4.1.4

Table 13: BlackDiamond 12804 Switch SFP Support

SFP	ExtremeXOS Required
1000BX SFP	11.6.1.9
LX100 SFP	12.0.1.11

SFPs supported on the BlackDiamond 12802 switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 14: BlackDiamond 12802 Switch SFP Support

SFP	ExtremeXOS Required
SX SFP	12.0.1.11
LX SFP	12.0.1.11
ZX SFP	12.0.1.11
1000BASE-T SFP	12.0.1.11
1000BX SFP	12.0.1.11
LX100 SFP	12.0.1.11

SFPs supported on the Summit X150 series of switches with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 15: Summit X150 Series Switches SFP Support

SFP	ExtremeXOS Required
100BASE-FX (for FE ports)	12.0.2.18
100BASE-BX SFP	12.0.2.18
100BASE LX10 SFP	12.0.2.18
SX SFP	12.0.2.18
LX SFP	12.0.2.18
ZX SFP	12.0.2.18
LX100 SFP	12.0.2.18
1000BX SFP	12.0.2.18

SFPs supported on the Summit X450 switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 16: Summit X450 Switch SFP Support

SFP	ExtremeXOS Required
10/100/1000BASE-T Copper SFP **Note:** Not supported on combo ports.	12.0.2.18
SX SFP	11.2.2.4
LX SFP	11.2.2.4
ZX SFP	11.2.2.4
100FX SFP **Note:** Not supported on combo ports.	11.4.3.4 or 11.5.2.8 (not supported in 11.5.1.4)

Table 16: Summit X450 Switch SFP Support

SFP	ExtremeXOS Required
100FX/1000LX SFP **Note:** Not supported on combo ports.	11.3.1.3
LX100 SFP	12.0.1.11
1000BX SFP	11.6.1.9

SFPs supported on the Summit X450a switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 17: Summit X450a Switch SFP Support

SFP	ExtremeXOS Required
10/100/1000BASE-T Copper SFP **Note:** Not supported on combo ports.	12.0.2.18
SX SFP	11.2.2.4
LX SFP	11.2.2.4
ZX SFP	11.2.2.4
100FX SFP **Note:** Not supported on combo ports.	11.6.1.9
100FX/1000LX SFP • Summit X450a-24x, ports 1 through 20	11.6.1.9
LX100 SFP	12.0.1.11
1000BX SFP	11.6.1.9

SFPs supported on the Summit X450e switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 18: Summit X450e Switch SFP Support

SFP	ExtremeXOS Required
SX SFP	11.6.1.9
LX SFP	11.6.1.9
ZX SFP	11.6.1.9
LX100 SFP	12.0.1.11
1000BX SFP	11.6.1.9

SFPs supported on the Summit X250e-24X switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 19: Summit X250e-24X SFP Support

SFP	ExtremeXOS Required
SX SFP, ports 25 and 26	12.0.2.18
LX SFP, ports 25 and 26	12.0.2.18
ZX SFP, ports 25 and 26	12.0.2.18
LX100 SFP, ports 25 and 26	12.0.2.18

Table 19: Summit X250e-24X SFP Support

SFP	ExtremeXOS Required
1000BX SFP, ports 25 and 26	12.0.2.18
100BASE FX (FE ports) SFP, ports 1 through 26	12.0.2.18
100BASE BX SFP, ports 1 through 26	12.0.2.18
100BASE LX10 SFP, ports 1 through 26	12.0.2.18

XENPAK Module Support

XENPAK modules supported on the BlackDiamond 8800 series of switches with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 20: BlackDiamond 8800 Series of Switches XENPAK Support

XENPAK Module	ExtremeXOS Required
LR	11.1.1.9
ER	11.1.1.9
SR	11.1.1.9
LX4	11.3.1.3
ZR	11.3.1.3

XENPAK modules supported on the BlackDiamond 10808 switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

11.4.1
Table 21: BlackDiamond 10808 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
LR	11.1.1.9
ER	11.1.1.9
SR	11.1.1.9
LX4	11.3.1.3
ZR	11.3.1.3
LW	11.4.1.4

XENPAK modules supported on the BlackDiamond 12804 switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 22: BlackDiamond 12804 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
LR	11.4.1.4
ER	11.4.1.4
SR	11.4.1.4
LX4	11.4.1.4
ZR	11.4.1.4
LW	11.4.1.4

XENPAK modules supported on the BlackDiamond 12802 switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include

Table 23: BlackDiamond 12802 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
LR	12.0.1.11
ER	12.0.1.11
SR	12.0.1.11
LX4	12.0.1.11
ZR	12.0.1.11
LW	12.0.1.11

XENPAK modules supported on the Summit X450 switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 24: Summit X450 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
SR	11.3.1.3
LR	11.3.1.3
ER	11.3.1.3
LX4	11.3.1.3
ZR	11.3.1.3

XENPAK modules supported on the Summit X450a switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 25: Summit X450a Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
SR	11.6.1.9
LR	11.6.1.9
ER	11.6.1.9
LX4	11.6.1.9
ZR	11.6.1.9
LW	11.6.1.9

XENPAK modules supported on the Summit X450e switch with ExtremeXOS 12.0, and the minimum ExtremeXOS version required, include:

Table 26: Summit X450e Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
SR	11.5.1.4
LR	11.5.1.4
ER	11.5.1.4
LX4	11.5.1.4

Table 26: Summit X450e Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
ZR	11.5.1.4

XENPAKs not supplied by Extreme Networks will show up as "Unsupported Optic Module" in the `show port x:y` information detail and `show port x:y configuration` command output.

XFP Module Support

XFP modules supported on the BlackDiamond 8800 series of switches with ExtremeXOS 12.0, the minimum ExtremeXOS version required include:

Table 27: BlackDiamond 8800 Series of Switches XFP Support

XFP Module	ExtremeXOS Required
SR	11.6.1.9
LR	11.6.1.9
ER	12.0.2.18

XFP modules supported on the Summit X450a and X450e series switch with ExtremeXOS 12.0, the minimum ExtremeXOS version required, and the manufacturers supported include:

Table 28: Summit X450a and X450e Series Switch XFP Support

XFP Module	ExtremeXOS Required
SR	11.5.1.4
LR	11.5.1.4
ER	12.0.2.18

Summit X150 Series Switch Software Details

The Summit X150 series switches have a reduced feature set as compared to the Summit X250 series switches. This section provides details of the software support for the Summit X150 series switches.

ExtremeXOS 12.0.2 (or later) Required

The Extreme Networks Summit X150 series switches are shipped with a manufacturing version of ExtremeXOS. This software version is not suitable for use in your network.

You must upgrade the software to the final release build of ExtremeXOS 12.0.2.18 (or later).

CAUTION

ExtremeXOS software builds earlier than version 12.0.2 do not support the Summit X150 series switches.

The switch may not work properly in your network if you install the switch without upgrading the software.

NOTE

This release is specifically designed and intended for the Summit X150 series switch only. You may only load this software on the specific Summit X150 series switch if you are authorized to do so. Authorization is defined as users possessing either an Extreme Networks Service Contract with a valid entitlement, or the product is still under the 90-day software warranty.

ExtremeXOS Command Line Support

The following is true for all Summit X150 series switches:

- Summit X150 series switches do not support L3 functionality; this platform does not support CLI commands for L3 functionality.
- Summit X150 series switches do not support stacking; all CLI commands for stacking are not supported on this platform.
- Summit X150 series switches do not support IP forwarding; however, CLI commands which configure IP addresses function in order to support accessing the management functionally of the switch.
- Upgrade or trial licensing is not available on the Summit X150 series switches.

Supported Commands on the Summit X150 Series Switches

Table 29 contains the list of CLI commands supported on the Summit X150 series switches.

Table 29: Summit X150 Supported Commands

Command	Description
check	Check policy syntax
policy	Policy
clear	Clear system configuration
access-list	Access list
account	Login account
counters	Statistics
cpu-monitoring	CPU utilization
debug	Debug command
eaps	Ethernet Automatic Protection Switching
elrp	ELRP (Extreme Loop Recovery Protocol)
elsm	ELSM (Extreme Link Status Monitoring)
esrp	ESRP (Extreme Standby Router Protocol)
fdb	FDB
igmp	IGMP Protocol
inline-power	Inline-Power
ip-security	IP Security
iparp	IP ARP command

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
ipmc	IPMC HELP
l2stats	Layer 2 stats
lacp	Link Aggregation Control Protocol
license-info	License information in EEPROM
log	Clear log message for memory-target
mld	Multicast Listener Discovery Protocol
neighbor-discovery	IPv6 neighbor
netlogin	Show Network Login specific information
session	Session
sys-recovery-level	Clear persistent sys-recovery-level
vlan	VLAN
<esrpDomain>	ESRP domain name
<vlan_name>	VLAN name
configure	Configure running system information
access-list	Access list
account	Login account
banner	System login banner
bootprelay	Configure BOOTP relay service
cli	CLI
cpu-transmit-priority	CPU transmit priority
debug	Debug information, core files
diffserv	Diffserv
dns-client	DNS Client
dos-protect	Automatic denial-of-service protection
dot1p	Dot1p
eaps	EAPS (Ethernet Automatic Protection Switching)
edp	EDP
egress	Egress
elrp-client	ELRP (Extreme Loop Recovery Protocol) Client
elsm	ELSM (Extreme Link Status Monitoring)
esrp	ESRP (Extreme Standby Router Protocol)
failsafe-account	Configure the failsafe account
fdb	FDB
forwarding	Configure settings for hardware forwarding
idletimeout	Timeout for idling configuration session
igmp	IGMP
inline-power	Inline-Power
ip-mtu	IP Maximum Transmission Unit
ip-security	IP Security
iparp	IP ARP command
jumbo-frame-size	Jumbo-frame-size

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
lacp	LACP (Link Aggregation Control Protocol)
lldp	Configure LLDP specific settings
log	Configure log service
mac-lockdown-timeout	MAC lockdown timeout
meter	Ingress traffic metering
mirroring	Mirroring
mld	Multicast Listener Discovery Protocol
mstp	MSTP configuration
mvr	Multicast VLAN Registration
neighbor-discovery	IPv6 neighbor
netlogin	Configure Network Login specific settings
ports	Ports
protocol	Protocol filter
qosprofile	QoS profile
qosscheduler	Set the QOS scheduling algorithm
radius	Configure Radius Server
radius-accounting	Configure Radius Accounting Server
safe-default-script	Safe default script configuration
sflow	Disable SFLOW module
sharing	Sharing
snmp	SNMP HELP
snmpv3	Configure SNMPv3
sntp-client	Configure SNTP Client
ssl	SSL
stpd	STP domain
sys-health-check	System health check
sys-recovery-level	Recovery level on exception
syslog	Remote syslog target
tacacs	Configure TACACS+ Server
tacacs-accounting	Configure TACACS+ Accounting Server
telnet	Telnet daemon
time	System time
timezone	Time zone
trusted-ports	Trusted ports
trusted-servers	Trusted servers
tunnel	Tunnel
vlan	VLAN
vman	vMAN configuration
<eapsDomain>	EAPS domain name
<esrpDomain>	ESRP domain name
<metername>	Meter name

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
<qosprofile>	QoS profile
<stpd_name>	STP domain name
<tunnel_name>	Tunnel name
<vlan_name>	VLAN name
cp	Copy file
internal-memory	Location is internal storage
<old-name>	Old file name
create	Create system configuration
access-list	Dynamic rule
account	Login account
eaps	EAPS (Ethernet Automatic Protection Switching) domain
fdbentry	FDB entry
log	Configure log service
meter	ingress traffic metering
netlogin	Netlogin
protocol	Protocol
qosprofile	QoS Profile
stpd	STP domain
tunnel	Tunnel
vlan	VLAN configuration
vman	vMAN configuration
debug	Reserved for debugging by Extreme Networks personnel
aaa	LLDP related debug commands
cfgmgr	Configuration Manager
cli	CLI information
devmgr	Device manager
ds	Directory Services
eaps	EAPS (Ethernet Automatic Protection Switching)
ems	Event Management Service (ems)
epm	Extreme Process Manager
hal	HAL debug hook
msgsrv	MSGSRV HELP
nodemgr	Node Manager module
snmpmaster	SNMPMASTER HELP
stp	Spanning Tree Protocol
telnetd	Telnet daemon
tftpd	TFTP daemon
thttpd	THTTPD daemon
vlan	VLAN
xmld	XML API daemon
delete	Delete system configuration

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
access-list	Access-list
account	Login account
eaps	EAPS (Ethernet Automatic Protection Switching) domain
esrp	ESRP (Extreme Standby Router Protocol) domain
fdbentry	FDB entry
log	Configure log service
meter	Ingress traffic metering
netlogin	Netlogin
protocol	Protocol
qosprofile	QoS profile
stpd	STP domain
tunnel	Tunnel
vlan	VLAN configuration
vman	vMAN configuration
<eapsDomain>	EAPS domain name
<metername>	Meter name
<stpd_name>	STP domain name
<tunnel_name>	Tunnel name
<vlan-name>	VLAN name
disable	Disable running system setting
access-list	Access list
bootp	Configure BOOTP client
bootprelay	Enable bootp relay service
cli	CLI settings
cli-config-logging	CLI command logging
clipaging	Display command output one screen at a time
cpu-monitoring	Monitor system/process CPU utilization
dhcp	Configure DHCP client
diffserv	Diffserv
dos-protect	Automatic denial-of-service protection
dot1p	Dot1p
eaps	EAPS (Ethernet Automatic Protection Switching) domain
edp	EDP
elrp-client	ELRP (Extreme Loop Recovery Protocol) Client
elsm	ELSM (Extreme Link Status Monitoring)
flooding	Flooding
icmp	ICMP option
idletimeout	Timeout for idling configuration session
igmp	IGMP Protocol
inline-power	Inline-Power
ip-option	IP option

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
ip-security	IP Security
iparp	IP ARP command
iproute	IPROUTE HELP
jumbo-frame	Jumbo-frame
learning	Learning
lldp	Configure LLDP specific settings
log	Configure log service
loopback-mode	Loopback
mac-lockdown-timeout	MAC lockdown timeout
mirroring	Mirroring
mld	Multicast Listener Discovery Protocol
mvr	Multicast VLAN Registration
netlogin	Configure Network Login specific settings
ports	Port
radius	RADIUS Client
radius-accounting	RADIUS Client Accounting
rmon	RMON CLI command
sflow	Disable sFlow module
sharing	Sharing
smartredundancy	Smart redundancy on a port (software redundant feature)
snmp	Configure SNMP specific settings
sntp-client	Enable SNTP client
stpd	STP domain
syslog	Configure syslog service
tacacs	TACACS+ Client
tacacs-accounting	TACACS+ Client Accounting
tacacs-authorization	TACACS+ Client Cli Authorization
telnet	Disable incoming telnet connections
udp-echo-server	Enable a UDP-Echo Server
vlan	VLAN configuration
watchdog	Watchdog monitoring feature
web	WEB HELP
xml-cli	CLI-based XML configuration mode
xml-mode	Raw XML configuration mode
<eapsDomain>	EAPS domain name
<stpd_name>	STP domain name
<vlan-name>	VLAN name
download	Download system image
bootrom	BootROM
image	Image
ssl	SSL

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
edit	Edit file
policy	Policy
script	XOS CLI script
enable	Enable running system setting
access-list	Access list
bootp	Configure BOOTP client
bootprelay	Enable BOOTP relay service
cli	CLI settings
cli-config-logging	CLI command logging
clipaging	Display command output one screen at a time
cpu-monitoring	Monitor system/process CPU utilization
dhcp	Configure DHCP client
diffserv	Diffserv
dos-protect	Automatic denial-of-service protection
dot1p	Dot1p
eaps	EAPS (Ethernet Automatic Protection Switching) domain
edp	EDP
elrp-client	ELRP (Extreme Loop Recovery Protocol) Client
elsm	ELSM (Extreme Link Status Monitoring)
esrp designated-carrier	ESRP designated carrier feature
flooding	Flooding
icmp	ICMP option
idletimeout	Timeout for idling configuration session
igmp	IGMP Protocol
inline-power	Inline-Power
ip-option	IP option
ip-security	IP security
iparp	IP ARP command
iproute	IPROUTE HELP
jumbo-frame	Jumbo-frame
learning	Learning
license	ExtremeXOS license or feature pack
lldp	Configure LLDP specific settings
log	Configure log service
loopback-mode	Loopback
mac-lockdown-timeout	MAC lockdown timeout
mirroring	Mirroring
mld	Multicast Listener Discovery Protocol
mvr	Multicast VLAN Registration
netlogin	Configure Network Login specific settings
ports	Port

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
radius	RADIUS Client
radius-accounting	RADIUS Client Accounting
rmon	RMON CLI command
sflow	Enable SFLOW module
sharing	Sharing
smartredundancy	Smart redundancy on a port (software redundant port feature)
snmp	Configure SNMP specific settings
sntp-client	Enable SNTP client
stpd	STP domain
syslog	Configure syslog service
tacacs	TACACS+ Client
tacacs-accounting	TACACS+ Client Accounting
tacacs-authorization	TACACS+ Client Cli Authorization
telnet	Allow incoming telnet connections
udp-echo-server	Enable a UDP-Echo Server
vlan	VLAN configuration
watchdog	Watchdog monitoring feature
web	WEB HELP
xml-cli	CLI-based XML configuration mode
xml-mode	Raw XML configuration mode
<eapsDomain>	EAPS domain name
<stpd_name>	STP domain name
<vlan-name>	VLAN name
exit	Exit configuration shell
history	Command history
install	Install system image
bootrom	Package to install
image	Package to install
jerry	Hidden debug command
aaa	LLDP related debug commands
acl	ACL debug agent
clear	CLEAR HELP
clear-flow	CLEAR-Flow agent
configure	Configure running system information
create	Create CPU FDB entry
delete	Delete CPU FDB entry
disable	None
ds	DS process
elsm	ELSM (Extreme Link Status Monitor)
ems	Event Management Service (ems)
enable	Enable system debug settings

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
exsh-var	Exsh session variable
force_synchronize	Force sync to backup MSM, which booted manually from pmon
hal	HAL debug hook
ip-security	IP Address security debug commands
iproute	IP ROUTE HELP
lacp	LACP (Link Aggregation Control Protocol)
lldp	LLDP related debug commands
load	Load system configuration
mcm	MCM HELP
modify	MODIFY HELP
netlogin	Network Login related debug commands
nettools	Configure/show netTools related information
policy-client	Policy Manager Client Test
policy-client-get	POLICY-CLIENT-GET HELP
printk	Kernel debugging printk
refresh	Refresh policy/policies
rmon	RMON debug information
run	Run soap operation
save	Save Policy in Policy Manager Memory
set	Set system configuration
sflow	sFlow module
show	Show running system information
start	Initiate operation
unconfigure	UNCONFIGURE HELP
upload	Upload hidden files to tftp server
validate	Validate and expand a string
xml-test	XML parsing library test
xx_force_synchronize	Do not use - part of synchronize macro without checks
xx_synchronize	Do not use - part of internal sync macro
xx_synchronize2	Do not use - part of internal sync macro
load	Load system configuration
script	ExtremeXOS CLI script
logout	Exit configuration shell
ls	List file
internal-memory	Internal CF
mv	Rename file
internal-memory	Location is internal storage
<old-name>	Old file name
nslookup	Get IP address of host
<host-name-or-ip>	Host name or IP address
ping	Ping an IP address

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
continuous	Ping the specified host until stopped
count	Number of ping requests to send
dont-fragment	Set the IP do not fragment bit
interval	Time interval between sending out ping request
ipv4	Force use of IPv4 transport
ipv6	Force use of IPv6 transport
start-size	Start size of the ping packets to send
tos	Set the TOS value
ttl	Set the TTL value
udp	Use an UDP ping instead of ICMP ping
vr	Ping from specified virtual router
<host>	Host to ping
quit	Exit configuration shell
reboot	Reboot system
cancel	Cancel scheduled reboot
time	Scheduled reboot
refresh	Refresh system configuration
policy	Policy
reset	Reset
inline-power	Inline-Power
restart	Restart device
ports	Ports
process	Process
rm	Remove file
internal-memory	File from internal storage
<file-name>	Name of the file to delete
rtlookup	Look up route to an IP address
<ipaddress>	Destination address
<ipv6address>	Destination address
run	Start new process
diagnostics	Perform diagnostics test
elrp	ELRP (Extreme Loop Recovery Protocol)
update	Read epmrc configuration file
save	Save system configuration
configuration	System configuration
primary	Primary configuration file
secondary	Secondary configuration file
show	Show running system information
access-list	Access list
accounts	Show accounts
banner	System login banner

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
bootprelay	Show the BOOTP relay information
checkpoint-data	Checkpoint data
configuration	System configuration
cpu-monitoring	CPU utilization statistics
debug	Debug info
dhcp-client	Show information related to dhcp-clients
dhcp-server	Show information related to the dhcp-server
diagnostics	Show diagnostic test results
diffserv	Diffserv
dns-client	Show configuration
dos-protect	Automatic denial-of-service protection
dot1p	Dot1p
dot1q	IEEE 802.1Q
eaps	Ethernet Automatic Protection Switching
edp	EDP information
elrp	ELRP (Extreme Loop Recovery Protocol)
elsm	ELSM (Extreme Link Status Monitoring)
esrp	ESR (Extreme Standby Router Protocol)
failsafe-account	Show the failsafe account information
fans	Fan information
fdb	FDB
forwarding	Show settings for hardware forwarding
heartbeat	Monitor process health
igmp	IGMP Protocol
inline-power	Inline-Power
ip-security	IP Security
iparp	IP ARP command
ipconfig	IP configuration
ipmroute	IP multicast routing module
iproute	IP routing module
ipstats	IP statistics
l2stats	Layer 2 stats
lacp	Link Aggregation Control Protocol
licenses	Switch licenses
lldp	Configure LLDP specific settings
log	Show information related to logging
mac-lockdown-timeout	MAC lockdown with timeout
management	Management
memory	Memory statistics
meter	METER HELP
mirroring	Mirroring

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
mld	Multicast Listener Discovery Protocol
mvr	Multicast VLAN Registration
neighbor-discovery	IPv6 neighbor
netlogin	Show Network Login specific information
node	Node
odometers	Odometers
policy	Policy
ports	Ports
power	Power information
process	Process information
protocol	Protocol
qosprofile	QoS profile
radius	RADIUS and radius accounting configuration
radius-accounting	RADIUS Client Accounting
rmon	RMON CLI command
session	Show active sessions
sflow	Show sFlow configuration
snmpv3	SNMPv3
sntp-client	Show configuration and statistics
ssl	SSL setup
stpd	STP domain
switch	Switch information
tacacs	TACACS+ configuration
tacacs-accounting	TACACS+ Client Accounting
tech	Technical support information
temperature	Temperature
tunnel	Tunnel
udp-echo-server	Show the UDP-Echo Server configuration
udp-profile	UDP forwarding profile
version	Version information
vlan	VLAN
vman	vMAN
<eapsDomain>	EAPS domain name
<name>	ESRP domain name
<stpd_name>	STP domain name
<vlan_name>	VLAN name
start	Start process
process	Process
telnet	Telnet client
vr	Virtual router
<host_name>	Remote host name

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
<remote_ip>	Remote telnet server IP address
terminate	Terminate running process
process	Process information
tftp	TFTP client
get	Get file
put	Put file
<host-name>	Remote TFTP server host name
<ip-address>	Remote TFTP server address
top	Display system utilization
traceroute	Trace route to an IP address
ipv4	Force use of IPv4 transport
ipv6	Force use of IPv6 transport
vr	Traceroute from virtual router ID
<host>	IPv4 host to traceroute
unconfigure	Unconfigure system configuration
access-list	Access list
bootprelay	BOOTP relay agent information option
diffserv	Diffserv
eaps	EAPS (Ethernet Automatic Protection Switching)
elrp-client	ELRP (Extreme Loop Recovery Protocol) Client
icmp	ICMP option
igmp	IGMP
inline-power	Inline-power
iparp	IP ARP command
irdp	ICMP Router Discovery Protocol
lldp	Configure LLDP specific settings
log	Configure log service
mld	Multicast Listener Discovery Protocol
mstp	MSTP configuration
netlogin	Configure Network Login specific settings
ports	Port
qosprofile	QoS profile
radius	Unconfigure RADIUS Server
radius-accounting	Unconfigure RADIUS Accounting Server
sflow	Unconfigure sFlow port
sntp-client	Unconfigure SNTP client
stpd	STP domain
switch	Switch configuration
tacacs	Unconfigure TACACS+ Server
tacacs-accounting	Unconfigure TACACS+ Accounting Server
trusted-ports	Trusted ports

Table 29: Summit X150 Supported Commands (Continued)

Command	Description
tunnel	Tunnel
vlan	VLAN
vman	vMAN
<eapsDomain>	EAPS domain name
<stpd_name>	STP domain name
<tunnel_name>	Tunnel name
<vlan_name>	VLAN name
uninstall	Uninstall system image
image	Package to uninstall
upload	Upload system configuration
configuration	System configuration
debug	Transfer support/debug data out of the switch
log	Show information related to logging
use	Select system configuration
configuration	System configuration
image	Package to run
vi	Invoke ExtremeXOS CLI editor
<filename>	ExtremeXOS CLI file name

Unsupported Commands on the Summit X150 Series Switches

Following is the list of processes that are not moved from Edge license to L2 Edge license.

- bgp
- msdp
- ospf
- ospfv3
- rip
- ripng
- pim
- vrrp
- brm
- upm

Table 30 lists the CLI commands not supported on the Summit X150 series switches.

Table 30: Summit X150 Unsupported Commands

Command	Description
>configure	Configure running system information
ipforwarding	Configure IP forwarding behavior
ipmcforwarding	Configure IP multicast forwarding parameters

Table 30: Summit X150 Unsupported Commands (Continued)

Command	Description
ipmroute	IP multicast routing module
irdp	ICMP Router Discovery Protocol
stacking	Settings for stacking
vlan {vlan_name} router-discovery	IPv6 Router Discovery
vlan {vlan_name} udp-profile	UDP Forwarding profile
disable	Disable running system setting
esrp	ESRP (Extreme Standby Router Protocol) Domain
ipforwarding	IP forwarding
ipmcforwarding	IPMCFORWARDING HELP
irdp	ICMP Router Discovery Protocol
router-discovery	IPv6 Router Discovery
stacking	Stacking
enable	Enable running system setting
esrp <esrp-domain>	ESRP (Extreme Standby Router Protocol) Domain
ipforwarding	IP forwarding
ipmcforwarding	IPMCFORWARDING HELP
irdp	ICMP Router Discovery Protocol
router-discovery	IPv6 Router Discovery
stacking	Stacking
reboot	Reboot system
node-address	Reboot a node in the stack
stack-topology	Reboot stack-topology
show	Show running system information
stacking	Stacking information
synchronize	Synchronize entire primary MSM to backup MSM
stacking	Synchronize stacking configuration
unconfigure	Unconfigure system configuration
stacking	Settings for stacking
vlan {vlan_name} router-discovery	IPv6 Router Discovery
vlan {vlan_name} udp-profile	UDP Forwarding profile

Tested Third-Party Products

This section lists the third-party products tested for ExtremeXOS 12.0.

Tested RADIUS Servers

The following RADIUS servers are fully tested:

- Microsoft—Internet Authentication Server

- Funk Software—Steel-Belted Radius Enterprise Edition 4.5
- Meetinghouse
- FreeRADIUS

Tested Third-Party Clients

The following third-party clients are fully tested:

- Funk Odyssey 2.2
- MeetingHouse Data AEGIS 2.0.5
- Odyssey 3.03.0.1194

Legacy IP Phones

The following wired IP phones have been verified for PoE power up only:

- Avaya 4620SW IP telephone
- Avaya one-X

PoE Capable VoIP Phones

The following PoE capable VoIP phones are fully tested:

- Avaya 4620SW IP telephone
- Avaya one-X

Extreme Switch Security Assessment

DoS Attack Assessment

The following third-party tools are used to assess DoS Attack Vulnerability:

- Network Mapper (NMAP)

ICMP Attack Assessment

The following third-party tools are used to assess ICMP Attack Vulnerability:

- SSPing
- Twinge
- Nuke
- WinFreeze

Port Scan Assessment

The following third-party tools are used to assess Port Scan Assessment:

- Nessus

2 Upgrading to ExtremeXOS 12.0

This chapter contains the following sections:

- Staying Current on page 45
- Upgrading ExtremeXOS on page 45
- Installing an ExtremeXOS Module on page 59
- Uninstalling an SSH Module on page 60
- Downgrading Switches on page 60

Staying Current

If you are an Extreme Assist customer, the latest release and release notes are available after logging in to the Tech Support web site at

http://www.extremenetworks.com/go/esupport.htm.

For more information about ExtremeXOS, see the *ExtremeXOS Concepts Guide* and the *ExtremeXOS Command Reference Guide*.

Upgrading ExtremeXOS

Upgrading your current ExtremeXOS installation to ExtremeXOS version 12.0 is a multistep process. In this section is a quick summary of the necessary steps, followed by detailed instructions.

NOTE

With ExtremeXOS 12.0.2.25, the BlackDiamond 12800 series switches now require a firmware upgrade along with the standard software upgrade.

NOTE

See the "Hitless Upgrade Caveats for the BlackDiamond 8800 Series Switch Only" in the ExtremeXOS Concepts Guide for an important caution about performing an MSM failover.

NOTE

A "Failed to install image" error occurs when trying to upgrade from ExtremeXOS 11.2.1 images to ExtremeXOS 11.6 or later. To upgrade to ExtremeXOS 11.6, you must currently be running ExtremeXOS 11.2.1 or later. If you are not running 11.2.1 or later you must first upgrade to ExtremeXOS 11.2.1 and then upgrade to ExtremeXOS 11.6.

NOTE

You can load ExtremeXOS software on the BlackDiamond 10808 series switch, the BlackDiamond 8800 family of switches, and the Summit X450 switch. BlackDiamond 8810 switches require version 11.1.1 or later, BlackDiamond 8806 switches require version 11.3.1 or later, BlackDiamond 12802 switches require version 12.0, BlackDiamond 12804 switches require version 11.4.1 or later, and the Summit X450 switches require a minimum of version 11.2.1. Summit X450a and Summit X450e series switches require ExtremeXOS 11.5 and higher.

Quick Summary

To install and upgrade to ExtremeXOS 12.0 on your system, you will be following these steps:

1 Download the image to your TFTP server.
2 Verify which virtual router connects to your TFTP server.
3 Save your configuration to a backup configuration file.
4 Determine your selected and booted image partitions.
5 Select the download partition and partition to use on reboot.
6 Download and install the image to the switch.
7 Reboot the switch.
8 Save the configuration for the new image.
9 Upgrade the BootROM—BlackDiamond 10808 switch only.
10 Upgrade the BootROM and PSU controller firmware--BlackDiamond 8800 family of switches only.
11 Upgrade the BootROM and PSU controller firmware--BlackDiamond 12804 family of switches only.

NOTE

If you have a dual MSM system, and the software image is not the same on both MSMs, see the section "Dual MSM Systems with Different Images Present" on page 58.

Detailed Steps

NOTE

Extreme Networks recommends using a TFTP server that supports blocksize negotiation (per RFC-2348). Using this type of server enables the switch to download the images faster.

To upgrade to ExtremeXOS 12.0 on your system, follow these steps:

1 Download the image to your TFTP server.

Download the image you received from Extreme Networks to your TFTP server.

2 Verify which virtual router connects to your TFTP server.

Use the following `ping` commands to test which virtual router you will need to specify when you download the image to your switch. This example assumes that your TFTP server's IP address is 192.168.0.12; substitute your own address when you issue the command:

```
ping vr vr-mgmt 192.168.0.12
```

```
ping vr vr-default 192.168.0.12
```

At least one of these commands must successfully reach your TFTP server for you to download the image. When you download the image in step 6, specify the virtual router that allowed you to reach your TFTP server.

3 Save your configuration to a backup configuration file.

You must save your configuration to a backup configuration file, or you will be unable to revert to your currently running image, if the need arises. In this example, we use the software version number as part of the name. Use the following command to save the configuration to the file *version11_6_1_7.cfg*:

```
save configuration version11_6_1_7
```

As an optional, extra precaution, we suggest that you save this configuration to a TFTP server. Use the `tftp` command to save your configuration. In the following example, the TFTP server's IP address is *192.168.0.12*, the virtual router determined in step 2 is *vr-mgmt*, and the configuration file is *version11_6_1_7.cfg*:

```
tftp 192.168.0.12 -v vr-mgmt -p -l version11_6_1_7.cfg
```

4 Determine your selected and booted image partitions.

Issue the `show switch` command to determine your current selected and booted image partitions. The selected image partition indicates which image will be used at the next reboot. The booted image partition indicates which image was used at the last reboot.

Output from this command includes the version of the selected and booted images and if they are in the primary or the secondary partition. In this example, the selected and booted images are in the primary partition.

```
...
Image Selected:      primary
Image Booted:        primary
Primary ver:         11.6.1.7
Secondary ver:       11.6.1.7

Config Selected:     primary.cfg
Config Booted:       primary.cfg
```

5 Select the download partition and partition to use on reboot.

Specify the partition by issuing the following command:

```
use image pri
```

OR

```
use image sec
```

6 Download and install the image to the switch.

Download and install the image to the switch using the `download image` command. The virtual router `<vr>` that you will use is the one you determined in step 2. This example assumes that you are using virtual router *vr-mgmt* and TFTP server *192.168.0.12*. Substitute your own virtual router and IP address when you issue the command:

```
download image 192.168.0.12 bd10k-12.0.2.25.xos vr vr-mgmt
```

(This may not be the actual filename; it is just an example.)

You will be asked:

```
Do you want to install image after downloading ? (y—yes, n—no, <cr>—cancel)
```

Answer *y*, for yes, so that the image will be installed after downloading.

7 Reboot the switch.

Use the `reboot` command to reboot the switch.

NOTE

For the BlackDiamond 8810 only—The first time the switch is rebooted after you upgrade to the 12.0 image, you will be prompted to upgrade the BootROM. Answer yes *to the prompt.*

8 Save the configuration for the new image.

Even though your configuration was saved before you rebooted, you will need to save the configuration with the new image. If you wait to login for some time after the reboot, you will receive a notice that recommends that you save the configuration. If you login soon after the reboot, you will not receive the notice, although an asterisk (*) will appear before the command prompt, indicating that the current configuration is not saved. In either case, save the configuration with the command:

```
save configuration
```

9 Upgrade the BootROM—BlackDiamond 10808 switch only.

Extreme Networks recommends that you upgrade to the latest BootROM for the BlackDiamond 10808. While not strictly required for this release, it is highly recommended. Run the `show version` command to verify the BootROM version currently running on your switch. If you are not running BootROM version 1.0.1.5 or later, upgrade the BootROM using the following command:

```
download bootrom 192.168.0.12 bd10k-1.0.1.5-bootrom.xbr
```

This example assumes that you will use the same TFTP server and virtual router as in step 6 above.

You will be asked if you want to install the BootROM after downloading. Answer yes, or use the `install bootrom` command to install later. Once the BootROM is downloaded and installed, it replaces the previous image stored in the onboard FLASH memory, and will be used at the next reboot.

10 Upgrade the BootROM and PSU controller firmware--BlackDiamond 8800 family of switches only.

NOTE

BootROMs installed by Manufacturing should never be forced to an earlier BootROM version unless explicitly instructed by Extreme Networks support.

Extreme Networks requires that you upgrade the MSMs, I/O modules, and PSU controllers in the BlackDiamond 8810 with the BootROM and firmware images included in this release of ExtremeXOS.

This release of ExtremeXOS contains the following versions of the BootROM and firmware:

MSM BootROM	1.0.1.11	First available in ExtremeXOS 12.0.1.11
I/O module BootROM	1.0.1.11	First available in ExtremeXOS 12.0.1.11
PSU controller firmware	2.13	First available in ExtremeXOS 11.4.1.4

Use the `show version` command to display the versions of the BootROM and firmware currently installed.

To install the new BootROM and firmware, wait until the `show slot` command indicates the MSMs and I/O modules are operational. Then use the `install firmware` command. This command will install the new BootROMs or firmware only on modules that have older BootROMs or firmware installed. You will be asked if you want to install each type of BootROM or firmware. New PSU controller firmware is used immediately after it is installed without rebooting the switch. The new BootROM and firmware overwrite the older versions stored in FLASH memory.

```
BD-8806.2 # install firmware
Installing version 1.0.1.11 of the MSM bootrom(s). Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Do you want to save configuration changes to primary.cfg? (y or n) Yes
Saving configuration on primary MSM ....... done!
Installing version 1.0.1.11 of the IO module bootrom(s). Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing version 2.13 of the PSU control module firmware. Do you want to
continue?
(y - yes, n - no, <cr> - cancel) Yes

Installing bootrom...

MSM bootrom(s) installed successfully
MSM bootrom(s) will be activated upon next MSM reboot
Installing bootrom...

IO module bootrom(s) installed successfully
IO module bootrom(s) will be activated upon next IO module reboot

Installing version 2.13 of the PSU control module firmware. Do you want to
continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing firmware...
PSU controller firmware installed successfully
BD-8806.3 #
```

11 Upgrade the BootROM and PSU controller firmware--BlackDiamond 12804 family of switches only.

NOTE

BootROMs installed by Manufacturing should never be forced to an earlier BootROM version unless explicitly instructed by Extreme Networks support.

Extreme Networks requires that you upgrade the MSMs, I/O modules, and PSU controllers in the BlackDiamond 12804 with the BootROM and firmware images included in this release of ExtremeXOS.

This release of ExtremeXOS contains the following versions of the BootROM and firmware:

MSM Bootloader	1.0.0.3	First available in ExtremeXOS 11.4.1.3
PSU controller firmware	2.13	First available in ExtremeXOS 11.4.1.4

Use the `show version` command to display the versions of the BootROM and firmware currently installed.

NOTE

For single MSM systems, reboot the switch using the `reboot` *command after the firmware installation is complete.*

To install the new BootROM and firmware, wait until the `show slot` command indicates the MSMs and I/O modules are operational. Then use the `install firmware` command. This command will install the BootROMs and/or firmware only on modules that have older BootROMs or firmware installed. Once this installation is complete, reboot the switch using the `reboot` command.

NOTE

For dual MSM systems, the `install firmware` *command cannot install all the necessary software while the MSM is primary. To completely install the firmware, an MSM failover is required. First, run the* `install firmware`

command on the primary MSM. When the installation is complete, issue the `run msm-failover` *command to allow the switch to failover to the secondary MSM. Run the* `install firmware` *command on the new primary MSM. To revert back to your original primary MSM, issue the* `run msm-failover` *command. Because two failovers are required for a dual-MSM firmware installation, you* ***will not*** *need to run the* `reboot` *command after executing the* `install firmware` *procedure.*

NOTE

Upgrading a BlackDiamond 12804 slot can take a minimum of six minutes per slot.

```
BD-12804.7 # install firmware
Installing version 1.0.0.2 of the MSM bootrom(s). Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing IO module firmware, a reboot is required. Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing version 2.13 of the PSU control module firmware. Do you want to
continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing micro controller image on backup MSM requires rebooting backup MSM. Do
you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing bootrom...
Installing bootstrap
Installing active bootrom
Installing system FPGA image
Installing bootstrap
Installing active bootrom
Installing system FPGA image

MSM bootrom(s) installed successfully
MSM bootrom(s) will be activated upon next MSM reboot
Installing bootrom...
Installing microcontroller firmware to slot 1 ...
Installing FGPA firmware to slot 1. This will takes a few minutes...
Installing microcontroller firmware to slot 2 ...
Installing FGPA firmware to slot 2. This will takes a few minutes...
Installing microcontroller firmware to slot 5 ...
Installing FGPA firmware to slot 5. This will takes a few minutes...
Installing microcontroller firmware to slot 6 ...
Installing FGPA firmware to slot 6. This will takes a few minutes...
```

To verify that your firmware upgrade on both the MSM and I/O modules has been successful, verify using the following command:

```
show version detail
```

```
BD-12804.1 # show version detail
Chassis    : 804030-00-05 07085-00026 Rev 5.0
Slot-1     : 804031-00-05 0706F-00200 Rev 5.0 uC: 5.00 FPGA: 5.0d
Slot-2     : 804031-00-05 0703F-00184 Rev 5.0 uC: 5.00 FPGA: 5.0d
Slot-5     : 804031-00-05 0703F-00185 Rev 5.0 uC: 5.00 FPGA: 5.0d
Slot-6     :
MSM-A : 804046-00-07 0706F-00117 Rev 7.0 BootROM: 1.0.0.3 IMG: 12.0.2.25  uC:
5.00 FPGA: 3.30
MSM-B      : 804046-00-07 0706F-00122 Rev 7.0 BootROM: 1.0.0.3     IMG: 12.0.2.25
uC: 5.00
```

```
PSUCTRL-1 : 700111-00-01 06525-00997 Rev 1.0 BootROM: 2.13
PSUCTRL-2 : 700111-00-01 06525-00909 Rev 1.0 BootROM: 2.13
PSU-1     : PS 2336 4300-00145 0641K-22897 Rev 1.0
PSU-2     : PS 2336 4300-00145 0641K-23307 Rev 1.0
PSU-3     : PS 2336 4300-00145 0641K-23266 Rev 1.0
PSU-4     :
PSU-5     :
PSU-6     :
Image    : ExtremeXOS version 12.0.2.25 v1202b25 by release-manager
on Tue Nov 6 22:56:10 PST 2007
BootROM : 1.0.0.3
BD-12804.2 #
```

Following is an example of the old FPGA version:

```
MSM =  3.2a
I/O = 5.07 or earlier
```

Following is an example of the new FPGA version:

```
MSM= 3.30
I/O = 5.0d
```

The backup MSM version is not shown until the MSM is made the primary MSM.

Upgrading ExtremeXOS on a Summit X150

Upgrade ExtremeXOS on a Summit X150 to ExtremeXOS 12.0.2 as follows:

1. Save your configuration to a backup configuration file using the `save configuration <configuration_file_name>` command.

   You must save your configuration to a backup configuration file in order to revert to your currently running image if the need arises.

2. Run the `show version` command to verify the BootROM version currently running on your switch.

   If you are not running BootROM version 1.0.3.1, upgrade the BootROM using the following command:

   `download bootrom <tftp server ipaddress> pmon_summit-1.0.3.1.xtr vr <vrname>`

3. Determine your current active image partition by running the `show switch` command. The Image Booted field shows the current active partition.

4. Download the ExtremeXOS 12.0.2.25 image to the alternate partition using the following command:

   `download image <ipaddress> <filename> vr <vrname> <image partition>`

   For example, if your current image is running in the primary partition, download the new image in the secondary partition:

   `download image 10.60.116.11 summitX-12.0.2.25.xos vr vr-mgmt secondary`

5. Run the `show switch` command again to determine that the image is downloaded into the partition you have specified.

6. Reboot the switch.

   Use the `reboot` command to reboot the switch.

7. When the switch comes up, run the `save configuration` command to save the configuration in the upgraded image.

Upgrading ExtremeXOS on a Summit X250e

Upgrade a Summit X250e to ExtremeXOS 12.0.2 as follows:

1 Save your configuration to a backup configuration file using the `save configuration <configuration_file_name>` command.

You must save your configuration to a backup configuration file in order to revert to your currently running image if the need arises.

2 Run the `show version` command to verify the BootROM version currently running on your switch. If you are not running BootROM version 1.0.3.0, upgrade the BootROM using the following command:

```
download bootrom 10.60.116.11 pmon_Combined_1_0_3_0.xtr vr vr-mgmt
```

3 Determine your current active image partition by running the `show switch` command. The Image Booted field shows the current active partition.

4 Download the ExtremeXOS 12.0.2 image to the alternate partition using the following command:

```
download image <ipaddress> <filename> vr <vrname> <image partition>
```

For example, if your current image is running in the primary partition, download the new image in the secondary partition:

```
download image 10.60.116.11 summitX-12.0.2.25.xos vr vr-mgmt secondary
```

5 Run the `show switch` command again to determine that the image is downloaded into the partition you have specified.

6 Reboot the switch.

Use the `reboot` command to reboot the switch.

7 When the switch comes up, run the `save configuration` command to save the configuration in the upgraded image.

Upgrading ExtremeXOS on a Summit X450

Upgrade a Summit X450 to ExtremeXOS 12.0.2 as follows:

1 Save your configuration to a backup configuration file using the `save configuration` command.

You must save your configuration to a backup configuration file in order to revert to your currently running image if the need arises.

2 Download the latest image to the switch.

Download the image to the switch using the `download image` command. Download ExtremeXOS 12.0 image `summitX-12.0.2.25.xos`.

3 Reboot the switch.

Use the `reboot` command to reboot the switch.

Upgrading an MSM-5 and MSM-5R to ExtremeXOS 12.0 on a BlackDiamond 12802

The BlackDiamond 12802 requires ExtremeXOS 12.0.2 or later to function properly. The MSM-5 or MSM-5R currently ships with an earlier version of ExtremeXOS. It can be installed in a BlackDiamond 12802 but must be upgraded to ExtremeXOS 12.0 or later before deploying the BlackDiamond 12802 in a production environment.

Upgrade the MSM-5 or MSM-5R to ExtremeXOS 12.0 as follows:

1 From the Extreme Networks eSupport website, download the ExtremeXOS 12.0.2 FCS image to your TFTP server.

When powered up, the BlackDiamond 12802 comes up as a BlackDiamond 12804. An error is displayed on the console and in the logs similar to the following:

```
Running Image ...

ohdGetChassisInfo: Incorrect Chassis type found, defaulting to BIATHLON
ohd_init_hw: Error determining chassis info
Starting Extremeware XOS 11.4.3b4
Copyright (C) 1996-2006 Extreme Networks.  All rights reserved.
Protected by US Patent Nos: 6,678,248; 6,104,700; 6,766,482; 6,618,388; 6,034,957;
6,859,438; 6,912,592; 6,954,436.

Error: Failed to connect CLI for 16 seconds!
login: admin
password:

ExtremeWare XOS
Copyright (C) 2000-2006 Extreme Networks. All rights reserved.
Protected by US Patent Nos: 6,678,248; 6,104,700; 6,766,482; 6,618,388; 6,034,957;
6,859,438; 6,912,592; 6,954,436.
================================================================================ BD-
12804.1 # show log
05/02/2007 00:27:10.81 <Info:HAL.Card.Info> MSM-A: Module in MSM-A is operational
05/02/2007 00:27:10.39 <Info:AAA.authPass> MSM-A: Login passed for user admin
through serial
05/02/2007 00:27:07.75 <Erro:Kern.Error> MSM-A: ohd_eeprom_read: Error reading
eeprom for slot 15 at offset 0
05/02/2007 00:27:07.75 <Erro:Kern.Error> MSM-A: ohd_eeprom_read: Error reading
eeprom for slot 15 at offset 0
05/02/2007 00:27:07.75 <Erro:Kern.Error> MSM-A: ohd_eeprom_access: Error accessing
device -1
```

2 Use the management VLAN virtual router to connect to your TFTP server by configuring an IP address on the management VLAN using the following command:

```
configure mgmt ipaddress 192.168.1.134/24
```

Enter a default gateway using the following command:

```
configure iproute add default 10.201.1.1. vr "VR-Mgmt"
```

NOTE

The default VLAN has no ports because it does not recognize the chassis.

3 Test which virtual router you will need to specify when you download the image to your switch by using the following command and your own IP address:

```
ping vr vr-mgmt 192.168.0.12
```

This command must successfully reach your TFTP server in order to download the image.

4 Download and install the image to the switch using the following command:

```
download image 192.168.0.12 bd12k-12.0.2.xos vr vr-mgmt
```

5 When the switch returns the following message:

```
Do you want to install image after downloading ? (y-yes, n-no, <cr>-cancel)
```

Answer "y" to install the image after downloading.

6 Use the `reboot` command to reboot the switch.

7 Run the `show switch` command. Verify that the `SysName` and `System Type` read `BD-12802`, and that the image is specified as `12.0.2.25`.

```
SysName:          BD-12802
SysLocation:
SysContact:       support@extremenetworks.com, +1 888 257 3000
System MAC:       00:04:96:31:A2:40
System Type:      BD-12802

SysHealth check:  Enabled (Normal)
Recovery Mode:    All
System Watchdog:  Enabled

Current Time:     Thu May  3 11:31:07 2007
Timezone:         [Auto DST Disabled] GMT Offset: 0 minutes, name is UTC.
Boot Time:        Thu May  3 11:26:38 2007
Boot Count:       11
Next Reboot:      None scheduled
System UpTime:    4 minutes 29 seconds

Slot:             MSM-A *
                  ------------------------
Current State:    MASTER

Image Selected:   secondary
Image Booted:     secondary
Primary ver:      12.0.0.13
Secondary ver:    12.0.2.25

Config Selected:  NONE
Config Booted:    Factory Default
```

Upgrading a BlackDiamond Series of Switches Using Hitless Upgrade

NOTE

You must be running ExtremeXOS 11.1.1.9 or later to use hitless upgrade on a BlackDiamond 10808 switch.

NOTE

You must be running ExtremeXOS 11.4.1 or later to use hitless upgrade on the BlackDiamond 8800 series switch.

NOTE

For the BlackDiamond 8800 series of switches, attempting a hitless upgrade to ExtremeXOS 12.0.2.25 from an earlier release may fail during the download process. If this occurs, use the normal software upgrade.

Upgrading the Active Partition Using Hitless Upgrade

Upgrade the active partition using hitless upgrade as follows:

1 Issue the `show switch` command to determine which MSM is the primary and which MSM is the backup.

2 In the following example MSM-B is the backup.

Execute the CLI command `download image 10.201.14.13 bd12k-12.0.2.25.xos msm b`

```
* BD-12804.9 # download image 10.201.14.13 bd12k-12.0.2.25.xos msm b
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
Yes
Downloading to MSM-A.....................................
Downloading to MSM-B.....................................
Checking for possibility of hitless upgrade ...
done with success
Image will be installed to the active partition, a reboot required.
Do you want to continue? (y/n) Yes
```

When the download is complete MSM-B will reboot.

3 When MSM-B is up, issue the `show switch` command.

- Verify that MSM-A is the master MSM, and MSM-B is the backup MSM and that BACKUP is followed by (In Sync).
- Verify that "Image Selected" and "Image Booted" are both set for secondary on both MSM.
- Verify that backup MSM-B displays new image version.

```
MSM:              MSM-A *           MSM-B
------------------------            ------------------------
Current State:    MASTER            BACKUP (In Sync)
Image Selected:   secondary         secondary
Image Booted:     secondary         secondary
Primary ver:      11.4.1.4          11.4.1.4
Secondary ver:    11.4.1.4          12.0.2.25
```

4 Issue the `run msm-failover` command from MSM-A. MSM-B becomes the master MSM and MSM-A will reboot.

5 Run the `show switch` command.

- Verify that MSM-B is the master and MSM-A comes up as the backup. MSM-A will not become "in sync" with MSM-B.

  Error messages related to conduits should be ignored.

- Verify that "Image Selected" and "Image Booted" are both set for secondary on both MSMs.

```
MSM               MSM-A             MSM-B *
------------------------            ------------------------
Current State:    BACKUP            MASTER
Image Selected:   secondary         secondary
Image Booted:     secondary         secondary
Primary ver:      11.4.1.4          11.4.1.4
Secondary ver:     11.4.1.4          12.0.2.25
```

6 Run the CLI command `download image 10.201.14.13 bd12k-12.0.2.25.xos msm a`

```
* BD-12804.9 # download image 10.201.14.13 bd12k-12.0.2.25.xos msm a
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
Yes
Downloading to MSM-A.....................................................
Downloading to MSM-B.....................................................
Checking for possibility of hitless upgrade ...
done with success
Image will be installed to the active partition, a reboot required. Do you want
to continue? (y/n) Yes
```

7 Once download completes MSM-A will reboot.

8 Once MSM-A comes up, run the `show switch` command.

- Verify that MSM-B is master and MSM-A comes up as the backup MSM, and displays (In Sync)
- Verify that "Image Selected" and "Image Booted" are both set for secondary on both MSMs.
- Verify that both MSMs display the new image version.

```
MSM:                MSM-A              MSM-B *
----------------------------      ---------------------------------
Current State:      BACKUP (In Sync)  MASTER
Image Selected:     secondary         secondary
Image Booted:       secondary         secondary
Primary ver:        11.4.1.4          11.4.1.4
Secondary ver:      12.0.2.25         12.0.2.25
```

9 Execute another `run msm-failover` so that MSM-A becomes the master. Run the `show switch` command to confirm.

```
MSM:                MSM-A *              MSM-B
----------------------------      ---------------------------------
Current State:      MASTER               BACKUP (In Sync)
Image Selected:     secondary            secondary
Image Booted:       secondary            secondary
Primary ver:        11.4.1.4             11.4.1.4
Secondary ver:      12.0.2.25            12.0.2.25
```

10 Run the `show version detail` command on MSM-A, which will display all of the I/O modules running the previous version (11.4.1.4) image, the MSMs however will be running the latest image. This version difference will cause no service disruption to the system as long as newer functionalities from the latest image is NOT used. However, it is highly recommended the I/O slot image is also consistent with the MSM version.

11 To upgrade the I/O module image to 12.0, run the `disable slot <slot number>` command followed by the `enable slot <slot number>` command. The `disable slot` command causes the I/O module to power down; the `enable slot` command causes the I/O module to power up.

CAUTION

Executing the `disable slot` *and* `enable slot` *commands will cause service disruption until the slot is completely operational.*

Upgrading the Alternate Partition Using Hitless Upgrade

Performing a hitless upgrade on the alternate partition allows you to revert to the previous image in case the upgrade is not successful. Upgrade the alternate partition using hitless upgrade as follows:

1 Issue the `show switch` command to determine which partition is the active partition and which partition is the alternate partition.

2 In the following example, the secondary image is the active partition. The download is performed on the primary image.

Execute the CLI command `download image 10.201.14.13 bd12k-12.0.2.25.xos primary`

```
* BD-12804.8 # download image 10.201.13.14 bd12k-12.0.2.25.xos primary
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
Yes
```

3 When the download is complete, run the `show switch` command to confirm the new image downloaded to the primary image.

4 Verify the following before rebooting the backup MSM:

- "Primary ver:" is the image to be downloaded.
- "Image Selected" is set to primary.

```
MSM:                MSM-A *             MSM-B
                    ------------------------------------
Current State:      MASTER              BACKUP (In Sync)
Image Selected:     primary             primary
Image Booted:       secondary           secondary
Primary ver:        12.0.2.25           12.0.2.25
Secondary ver:      11.4.1.4            11.4.1.4
```

5 Issue the `reboot` command to reboot MSM-B only.

```
reboot msm b
```

6 Run the `show switch` command to verify that:

- MSM-B is (In Sync) mode.
- "Image Selected" and "Image Booted" are both set for primary on the backup MSM.

```
MSM:                MSM-A *             MSM-B
                    ------------------------------------
Current State:      MASTER              BACKUP (In Sync)
Image Selected:     primary             primary
Image Booted:       secondary           primary
Primary ver:        12.0.2.25           12.0.2.25
Secondary ver:      11.4.1.4            11.4.1.4
```

7 Execute the `run msm-failover` command from the master MSM (MSM-A).

8 MSM-B becomes the master MSM, and MSM-A will reboot.

9 Run the `show switch` command to:.

- Verify that MSM-B is the master MSM and MSM-A is the backup MSM and displays (In Sync).
- Verify that "Image Selected" and "Image Booted" are set for primary on both MSMs.

```
MSM:                MSM-A               MSM-B *
                    ------------------------------------
Current State:      BACKUP (In Sync)    MASTER
Image Selected:     primary             primary
Image Booted:       primary             primary
```

10 Run the `run msm-failover` command again so that MSM-A becomes the master MSM.

11 Run the `show switch` command to confirm the master MSM is now MSM-A.

```
MSM:                MSM-A *             MSM-B
                    ------------------------------------
```

```
Current State:      MASTER          BACKUP (In Sync)
Image Selected:     primary         primary
Image Booted:       primary         primary
Primary ver:        12.0.2.25       12.0.2.25
Secondary ver:      11.4.1.4        11.4.1.4
```

Dual MSM Systems with Different Images Present

If you have a dual MSM system that has different images on the MSMs, you will need to modify the upgrade procedure. One situation where you might have different images installed is when you add an MSM that has been in storage to your chassis, either for the first time, or as a replacement. You will only need to do the following procedure if one of the MSMs is running an image earlier than 11.0.0, and the images are different on the two MSMs (earlier versions of the software are unable to automatically synch up the configurations).

Follow the directions for upgrading the switch, and continue with step 6. When you download the image, as described in step 6, Download and install the image to the switch., you will be asked:

```
Do you want to install image after downloading ? (y—yes, n—no, <cr>—cancel)
```

Answer *n*, for no, so that the image will not be installed after downloading.

Next, manually install the image, using the following command:

```
install image bd10k-12.0.2.25.xos
```

Now the two MSMs have the same image installed, but may not have the same configurations. Reboot the secondary MSM using one of the following commands:

`reboot msm b` (if you are running on MSM A)

`reboot msm a` (if you are running on MSM B)

Finally, save the configuration on both MSMs by using the command

```
save configuration
```

Using a Rev 10 (or later) BlackDiamond 10808 MSM-1 or MSM-1XL

NOTE

To use a Rev 10 (or later) MSM-1 or MSM-1XL module, you must upgrade both the active and alternate images with the latest ExtremeWare 11.1.3 (or later) software image.

To determine which version of MSM you have installed in your switch, use the `show version` command.

If you have a Rev 9 (or earlier) MSM, the `show version` command output will look like this:

```
MSM-A :804015-00-09 0414F-00728 Rev 9.0 BootROM: 1.0.1.5 IMG:
```

If you have a Rev 10 (or later) MSM, the `show version` command output will look like this:

```
MSM-A :804407-00-10 0505F-00429 Rev 10.0 BootROM: 1.0.1.5 IMG:
```

Complete `show version` command output with Rev 10 MSMs will look like this:

```
BD-10808.2 #
BD-10808.2 # show version
Chassis    : 804300-00-03 0324X-00026 Rev 3.0
MSM-A      : 804407-00-10 0505F-00429 Rev 10.0 BootROM: 1.0.1.5 IMG:
MSM-B      : 804407-00-10 0505F-00431 Rev 10.0 BootROM: 1.0.1.5 IMG:
Image      : ExtremeXOS version 11.1.3.3 v11133 by release-manager on Thu Mar 31
19:12:57 PST 2005
BootROM : 1.0.1.7
BD-10808.3 #
```

Installing an ExtremeXOS Module

An ExtremeXOS module has functionality that supplements a core image. You will download and install a module onto an already installed core image. The version number of the core image and the module must match. For example, the module *bd10k-12.0.2.25-ssh.xmod* can only be installed onto the core image *bd10k-12.0.2.25.xos*.

You can download and install the SSH module.

NOTE

You must terminate and restart the thttpd process before you can use SSL

Assuming that you have an installed and running ExtremeXOS 12.0 software on the active partition, follow these steps to install the module:

1 Download the module image to your TFTP server.

Download the image you received from Extreme Networks to your TFTP server.

2 Determine the active partition for your switch.

Issue the `show switch` command to determine your current selected and booted image partitions. The booted image partition indicates the currently active partition.

3 Download and install the module image to the active partition.

Download the image to the switch using the `download image` command. The `filename` for the only available module image is *bd10k-12.0.2.25-ssh.xmod*.

The virtual router `<vr>` that you will use is the one that connects to your TFTP server (you determined this in step 2, "Verify which virtual router connects to your TFTP server." in the upgrade procedure). Since the system virtual router names changed from release 10.1.2.17 to 11.2.3.3, the name will be different from that used to download the initial upgrade image. Use *vr-mgmt* for this step or *vr-default*.

This example assumes that you are using virtual router *vr-mgmt* and TFTP server *192.168.0.12*, substitute your own virtual router and IP address when you issue the command:

```
download image 192.168.0.12 bd10k-12.0.2.25-ssh.xmod vr vr-mgmt <partition>
(primary or secondary)
```

You will be asked:

```
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
```

Answer *y*, for yes, so that the image will be installed after downloading.

4 Issue the `run update` command.

Issue the following command:

```
run update
```

The `run update` command starts up the processes associated with the new module, and makes them available to the system. You should now be able to issue the commands associated with SSH2.

You can verify that the SSH2 module is running by issuing the following command:

show process

If SSH2 is running, you will see a process named *exsshd* listed. You can then configure and enable SSH2 on the switch.

You can also verify that the SSH2 module is installed by issuing the following command:

show management

If the SSH module is installed, you will see text similar to the following:

```
SSH access : Disabled (Key invalid, tcp port 22 vr all)
```

If the SSH module is not installed, you will see text similar to the following:

```
SSH Access : ssh module not loaded.
```

Uninstalling an SSH Module

To uninstall the SSH module you must first terminate the THTTPD process:

1 Issue the `terminate process thttpd graceful` command. This terminates the THTTPD process.

2 Issue the `uninstall image bd10k-12.0.2.25-ssh.xmod <partition> (primary or secondary)` command. This uninstalls SSH from your switch.

3 Restart the thttpd process using the `start process thttpd` command.

Downgrading Switches

Following are the instructions for downgrading your ExtremeXOS version 12.0.2.25 installation to a previous version. It is assumed that you saved your configuration using the 11.4.1 image, and that the 11.4.1 image is currently installed on the switch, on the non-booted partition.

NOTE

Do not downgrade a BlackDiamond 8810 switch to an image earlier than 11.1.1 or a Summit X450 switch to an image earlier than 11.2.1. Do not downgrade a BlackDiamond 8806 switch to an image earlier than 11.3.1.1. Do not downgrade a Summit X450a or X450e switch to an ExtremeXOS image earlier than 11.5.1.

To downgrade to the existing ExtremeXOS version 11.4.1 image on your system, you will be following these steps:

1 Determine your selected and booted image partitions.

Issue the `show switch` command to determine your current selected and booted image partitions. The selected image partition indicates which image will be used at the next reboot. The booted image partition indicates which image was used at the last reboot.

Output from this command includes the version of the selected and booted images and if they are in the primary or the secondary partition. In this example, the selected and booted images are in the secondary partition.

```
...
Image Selected:      secondary
Image Booted:        secondary
Primary ver:         11.4.1.4
Secondary ver:       12.0.2.25

Config Selected:     primary.cfg
Config Booted:       primary.cfg
```

2 Select the reboot partition.

Assuming that the 11.4.1 image is on the non-booted partition, if you are currently running the image booted from the primary partition, issue this command:

```
use image secondary
```

If you are currently running the image booted from the secondary partition, issue this command:

```
use image primary
```

3 Select the reboot configuration.

Select the configuration to be used after reboot with the `use configuration` command. Assuming you saved the 11.4.1 configuration as *bdversion11_4_1_4.cfg*, use the following command:

```
use configuration bdversion11_4_1_4
```

4 Verify the image and configuration selection.

Again, issue the `show switch` command. The output should show that the selected image is the 11.4.1 image that you are downgrading to, and the selected configuration is the one you saved before you installed the 12.0.2.25 image:

```
...
Image Selected:      primary
Image Booted:        secondary
Primary ver:         11.4.1.4
Secondary ver:       12.0.2.25

Config Selected:     bdversion11_4_1_4.cfg
Config Booted:       primary.cfg
...
```

5 Reboot the switch.

Use the command `reboot` to reboot the switch.

3 Limits

This chapter summarizes the supported limits in ExtremeXOS.

Supported Limits

The table below summarizes tested metrics for a variety of features, as measured in a per-system basis unless otherwise noted. These limits may change but represent the current status. The contents of this table supersede any values mentioned in the *ExtremeXOS Concepts Guide*.

NOTE

See the ExtremeXOS Concepts Guide for information on which features are supported on each platform; see the specific section that discusses the specific feature.

Table 31: Supported Limits

Metric	Product	Limit
Access lists (policies)—suggested maximum number of lines in a single policy file.	BlackDiamond 10808	300,000
	BlackDiamond 12800 series	300,000
Access lists (policies)—maximum number of rules in a single policy file.[a]	BlackDiamond 8800 series	
	Original series modules	
	(per GigE port)	128
	(per 10 GigE port)	1,016
	a-series modules	2,048
	e-series modules	1,024
	BlackDiamond 10808	30,000
	Summit X150	1,024
	Summit X250e	
	per port groups 1-24 and 25-48	1,024
	Summit X450	
	(per GigE port)	128
	(per 10 GigE port)	1,016
	Summit X450a	
	per port groups 1-24 and 25-48	2,048
	Summit X450e	
	per port groups 1-24 and 25-48	1,024
Access lists (masks)—maximum number of ACL masks per port.[b]	BlackDiamond 8800 series	16
	Summit X450	16

Metric	Product	Limit
Access lists (slices)—maximum number of field selectors for ACL slices.	BlackDiamond 8800 series a-series modules per port groups 1-12, 25-36 and 13-24, 37-48 e-series modules per port groups 1-12, 25-36 and 13-24, 37-48 Summit X150 Summit X250e per port groups 1-24 and 25-48 Summit X450a per port groups 1-24 and 25-48 Summit X450e per port groups 1-25	 16 8 8 8 16 8
AAA (local)—maximum number of admin and local user accounts.	All platforms	16
BGP (aggregates)—maximum number of BGP aggregates.	All platforms	256
BGP (networks)—maximum number of BGP networks.	All platforms	1,024
BGP (peers)—maximum number of BGP peers.	BlackDiamond 8800 series BlackDiamond 10808 (MSM-1XL) BlackDiamond 10808 (MSM-1) BlackDiamond 12800 series (MSM-5R) Summit X250e Summit X450 * With default keepalive and hold timers.	256* 512 256 256* 128* 128*
BGP (peer groups)—maximum number of BGP peer groups.	All platforms	64
BGP (policy entries)—maximum number of BGP policy entries per route policy.	All platforms	256
BGP (policy statements)—maximum number of BGP policy statements per route policy.	All platforms	1,024
BGP (unique routes)—maximum number of unique BGP routes (LPM entries is limited to support TCAM entries on a BlackDiamond 10808).	BlackDiamond 8800 series BlackDiamond 10808 (MSM-1XL) BlackDiamond 10808 (MSM-1) BlackDiamond 12800 series (MSM-5R) Summit X250e Summit X450	25,000 1,000,000 180,000 225,000 25,000 25,000

Metric	Product	Limit
BGP (non-unique routes)—maximum number of non-unique BGP routes (LPM entries is limited to support TCAM entries on a BlackDiamond 10808).	BlackDiamond 8800 series	25,000
	BlackDiamond 10808 (MSM-1XL)	2,000,000
	BlackDiamond 10808 (MSM-1)	900,000
	BlackDiamond 12800 series (MSM-5R)	500,000
	Summit X250e	25,000
	Summit X450	25,000
BOOTP/DHCP relay—maximum number of BOOTP or DHCP servers per virtual router.	All platforms	4
Jumbo frames—maximum size supported for jumbo frames, including the CRC.	All platforms	9,216
EAPS domains—maximum number of EAPS domains. Note: An EAPS ring that is being spatially reused cannot have more than four configured EAPS domains.	BlackDiamond 8800 series	64
	BlackDiamond 10808	128
	BlackDiamond 12800 series	128
	Summit series	32
EAPSv1 protected VLANs—maximum number of protected VLANs.	BlackDiamond 8800 series	2,000
	BlackDiamond 10808	4,000
	BlackDiamond 12800 series	4,000
	Summit X150 series	1,000
	Summit X250e	1,000
	Summit X450	1,000
EAPSv2 protected VLANs—maximum number of protected VLANs.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	4,000
	BlackDiamond 12800 series	4,000
	Summit series	500
ELSM (ports per VLAN)—maximum number of VLANs per port.	BlackDiamond 8800 series	5,000
	BlackDiamond 10808	5,000
	BlackDiamond 12800 series	5,000
ESRP groups—maximum number of ESRP groups.	All platforms	7
ESRP domains—maximum number of ESRP domains.	BlackDiamond 8800 series	64
	BlackDiamond 10808	128
	BlackDiamond 12800 series	64
	Summit X250e	64
	Summit X450	64
ESRP VLANs—maximum number of ESRP VLANs.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	3,000
	BlackDiamond 12800 series	3,000
	Summit X250e	1,000
	Summit X450	1,000
ESRP (maximum ping tracks)—maximum number of IP route tracks per VLAN.	All platforms	8
ESRP (IP route tracks)—maximum IP route tracks per VLAN.	All platforms	8

Metric	Product	Limit
ESRP (VLAN tracks)—maximum number of VLAN tracks per VLAN.	All platforms	1
Forwarding rate—maximum L2/L3 software forwarding rate.	BlackDiamond 8800 series (Mpps)	10,000 pps
	BlackDiamond 12800 series	16,000
	Summit X250e (Mpps)	10,000 pps
	Summit X450 (Mpps)	10,000 pps
FDB (maximum L2/L3 entries)—maximum number of MAC addresses/IP host routes.	BlackDiamond 10808	224,000
	BlackDiamond 12800 series	49,000
	BlackDiamond 12800 R-series	224,000
FDB (maximum L2 entries)—maximum number of MAC addresses.	BlackDiamond 8800 series	
	(per I/O module) (per system)	16,384 128,000
	Summit X150 series	8,192
	Summit X250e	8,192
	Summit X450	16,384
	Summit X450a	16,384
	Summit X450e	8,192
	SummitStack	128,000
Hierarchical QoS—maximum number of ingress-only traffic queues per unit. (For 20XTR, first 10 ports ranges from 1 to 10 are UNIT-I, second 10 ports ranges from 11 to 20 are UNIT-II, for 10 Gig slot each port is one UNIT.)	BlackDiamond 12800 R-series	20,000
Hierarchical QoS—maximum number of ingress traffic queues with egress shaping allowed per switch.	BlackDiamond 12800 R-series	20,000
Hierarchical QoS—maximum number of egress-only traffic queues allowed per switch.	BlackDiamond 12800 R-series	30,000
Hierarchical QoS—maximum number of traffic queues attach per port.	BlackDiamond 12800 R-series	4,000
IGMP sender—maximum number of IGMP senders on an L2 configuration.	BlackDiamond 8800 series	500
	BlackDiamond 10808	15,000
	BlackDiamond 12800 series	15,000
	Summit X150	500
	Summit X250e	500
	Summit X450	500
IGMP sender—maximum number of IGMP senders per switch.	BlackDiamond 8800 series[d]	1,000
	BlackDiamond 10808	15,000
	BlackDiamond 12800 series	15,000
	Summit X150	1,000
	Summit X250e[d]	1,000
	Summit X450[d]	1,000

Metric	Product	Limit
IGMPv2 subscriber—maximum number of L2/L3 IGMPv2 subscribers per switch.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	5,000
	BlackDiamond 12800 series	5,000
	Summit X150	1,000
	Summit X250e	1,000
	Summit X450	1,000
IGMPv2 subscriber—maximum number of subscribers per switch.	BlackDiamond 8800 series	10,000
	BlackDiamond 10808	30,000
	BlackDiamond 12800 series	30,000
	Summit X150	10,000
	Summit X250e	10,000
	Summit X450	10,000
IGMPv3 maximum source per group—maximum number of source addresses per group.	All platforms	250
IGMPv3 subscriber—maximum number of L2/L3 IGMPv3 subscribers per switch.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	5,000
	BlackDiamond 12800 series	5,000
	Summit X150	1,000
	Summit X250e	1,000
	Summit X450	1,000
IGMPv3 subscriber—maximum number of IGMPv3 subscribers per switch.	BlackDiamond 8800 series	10,000
	BlackDiamond 10808	30,000
	BlackDiamond 12800 series	30,000
	Summit X150	10,000
	Summit X250e	10,000
	Summit X450	10,000
IP ARP entries in software—maximum number of IP ARP entries in software.	BlackDiamond 8800 series	20,480
	BlackDiamond 10808	20,480
	BlackDiamond 12800 series	20,480
	Summit X150 series	4,096
	Summit X250e	4,096
	Summit X450	4,096
IPv4 host entries in hardware—maximum number of IPv4 ARP entries and remote IPv4 hosts in hardware.[d]	BlackDiamond 8800 series	8,189
	BlackDiamond 8810 a-series	8,189
	BlackDiamond 8810 e-series	2,045
	BlackDiamond 10808	224,000
	BlackDiamond 12800 series	49,000
	BlackDiamond 12800 R-series	224,000
	Summit X250e	2,048
	Summit X450	8,189
	Summit X450a	8,192
	Summit X450e	2,048

Metric	Product	Limit
IPv6 host entries in hardware—maximum number of IPv6 ARP entries in hardware.[d]	BlackDiamond 8810 a-series	4,094
	BlackDiamond 8810 e-series	1,022
	BlackDiamond 10808	112,000
	BlackDiamond 12800 series	24,500
	BlackDiamond 12800 R-series	112,000
	Summit X250e	1,024
	Summit X450a	4,096
	Summit X450e	1,024
IPv4 routes (LPM entries in hardware)— number of IPv4 routes in hardware.[c]	BlackDiamond 8800 series	25,000
	BlackDiamond 8810 a-series	12,000
	BlackDiamond 8810 e-series	460
	BlackDiamond 10808	256,000
	BlackDiamond 12800 series	229,000
	Summit X250e	460
	Summit X450	25,000
	Summit X450a	12,000
	Summit X450e	460
IPv6 routes (LPM entries in hardware)—number of IPv6 routes in hardware.[cL]	BlackDiamond 8810 a-series	6,000
	BlackDiamond 8810 e-series	230
	BlackDiamond 10808	114,500
	BlackDiamond 12800 series	114,500
	Summit X250e	230
	Summit X450a	6,000
	Summit X450e	230
IP router interfaces—maximum number of VLANs performing IP routing–excludes sub VLANs (IPv4 and IPv6 interfaces).	All platforms	512
IP static routes—maximum number of permanent IP routes.	All platforms	1,024
IP route sharing (maximum gateways)—maximum number of configurable gateways used by equal cost multipath static routes.	BlackDiamond 8800 series	2, 4, or 8
	Summit X250e	2, 4, or 8
	Summit X450	2, 4, or 8

Metric	Product	Limit
IP route sharing (total destinations)—maximum number of unique destinations used by multipath OSPF, OSPFv3, or static routes.	BlackDiamond 8800 series	
	(default maximum gateways of 4)	512
	(if maximum gateways is 2)	1,024
	(if maximum gateways is 8)	256
	BlackDiamond 8810 a-series	
	(default maximum gateways of 4)	512
	(if maximum gateways is 2)	1,024
	(if maximum gateways is 8)	256
	BlackDiamond 8810 e-series	
	(default maximum gateways of 4)	32
	(if maximum gateways is 2)	64
	(if maximum gateways is 8)	16
	BlackDiamond 10808	
	(with up to 8 gateways per destination)	7,136
	BlackDiamond 12800 series	
	(with up to 8 gateways per destination)	7,136
	Summit X250e	
	(default maximum gateways of 4)	32
	(if maximum gateways is 2)	64
	(if maximum gateways is 8)	16
	Summit X450	
	(default maximum gateways of 4)	512
	(if maximum gateways is 2)	1,024
	(if maximum gateways is 8)	256
	Summit X450 a-series	
	(default maximum gateways of 4)	512
	(if maximum gateways is 2)	1,024
	(if maximum gateways is 8)	256
	Summit X450 e-series	
	(default maximum gateways of 4)	32
	(if maximum gateways is 2)	64
	(if maximum gateways is 8)	16
Load sharing groups—maximum number of load share groups.	BlackDiamond 8800 series	
	with 10G4X	32
	without 10G4X	128
	BlackDiamond 10808	128
	BlackDiamond 12800 series	128
	Summit X150 series	32
	Summit X250e	32
	Summit X450	32
	SummitStack	
	with Summit X450-24t	32
	with Summit X450-24x	32
	without Summit X450-24t	128
	without Summit X450-24x	128

Metric	Product	Limit
Load sharing—maximum number of ports per load share group.	BlackDiamond 8800 series	8
	BlackDiamond 10808	16
	BlackDiamond 12800 series	16
	Summit X150 series	8
	Summit X250e	8
	Summit X450	8
Logged messages—maximum number of messages logged locally on the system.	All platforms	20,000
MAC-based security—maximum number of MAC-based security policies.	All platforms	1,024
MAC-in-MAC—maximum number of MAC FDB entries (MAC addresses on the local side) and MAC binding entries (MAC addresses on remote side).	BlackDiamond 10808	100,000
	BlackDiamond 12800 series	100,000
MAC-in-MAC—maximum number of regular VLANs (VLAN, vMAN, BVLAN). No VLAN tag duplication support.	BlackDiamond 10808	4,000
	BlackDiamond 12800 series	4,000
MAC-in-MAC—maximum number of VLANs. (VLAN, vMAN, BVLAN, and SVLAN). VLAN tag duplication support on SVLANs.	BlackDiamond 10808 (1G DRAM)	16,000
	BlackDiamond 12800 series (512 DRAM)	8,000
Mirroring (filters)—maximum number of mirroring filters.	All platforms	16
Mirroring (monitor port)—maximum number of monitor ports.	All platforms	1
Mirroring, one-to-many (filters)—maximum number of one-to-many mirroring filters.	BlackDiamond 10808	16
	BlackDiamond 12800 series	16
Mirroring, one-to-many (monitor port)—maximum number of one-to-many monitor ports.	BlackDiamond 10808	16
	BlackDiamond 12800 series	16
MPLS configured interfaces—maximum number of MPLS configured interfaces per switch.	BlackDiamond 10808	16
	BlackDiamond 12800 series	10
MPLS LDP peers—maximum number of MPLS LDP peers per switch.	BlackDiamond 10808	16
	BlackDiamond 12800 series	12
MPLS LDP adjacencies—maximum number of MPLS LDP adjacencies per switch.	BlackDiamond 10808	50
	BlackDiamond 12800 series	50
MPLS LDP labels—maximum number of MPLS LDP labels per switch.	BlackDiamond 10808	20,000
	BlackDiamond 12800 series	5,000
	BlackDiamond 12800 series (MSM-5)	5,000
	BlackDiamond 12800 series (MSM-5R)	18,000
MSDP active peers—maximum number of active MSDP peers.	BlackDiamond 8800 series	32
	BlackDiamond 10808	32
	BlackDiamond 12800 series	32
	Summit X450	16

Metric	Product	Limit
MSDP SA cache entries—maximum number of entries in SA cache.	BlackDiamond 8800 series	16,000
	BlackDiamond 10808	16,000
	BlackDiamond 12800 series	16,000
	Summit X450	8,000
MSDP maximum mesh groups—maximum number of MSDP mesh groups.	BlackDiamond 8800 series	8
	BlackDiamond 10808	8
	BlackDiamond 12800 series	8
	Summit X450	4
IP multinetting (secondary IP addresses)—maximum number of secondary IP addresses per VLAN.	All platforms	64
Multicast VLAN registration (MVR)—maximum number of senders.	BlackDiamond 8800 series	500
	BlackDiamond 10808	15,000
	BlackDiamond 12800 series	15,000
	Summit X150	500
	Summit X250e	500
	Summit X450	500
Network Login—maximum number of MAC-based Network Login clients per system.	BlackDiamond 8800 series (per module)	1,024
	Summit X250e (per system)	1,024
	Summit X450 (per system)	1,024
Network Login—maximum number of MAC-based VLANs supported for 4K clients. *Note: If MAC-based Network Login VLANs are enabled on a port, you cannot configure L2, L3, or L4 ACLs on the port.	BlackDiamond 12804	4,000
PIM—maximum mroutes—maximum number of IP multicast data streams.	BlackDiamond 8800 series[d]	1,000
	BlackDiamond 10808	12,000
	BlackDiamond 12800 series	12,000
	Summit X250e[d]	1,000
	Summit X450[d]	1,000
PIM-SSM (maximum multicast groups)—PIM-SSM maximum mroutes/maximum number of IP multicast data streams.	BlackDiamond 8800 series[d]	1,000
	BlackDiamond 10808	15,000
	BlackDiamond 12800 series	15,000
	Summit X250e[d]	1,000
	Summit X450[d]	1,000
OSPF adjacencies—maximum number of supported OSPF adjacencies.	BlackDiamond 8800 series	128
	BlackDiamond 10808	255
	BlackDiamond 12800 series	255
	Summit X250e	128
	Summit X450	128
OSPF areas—as an ABR, how many OSPF areas are supported within the same switch.	All platforms	8

Metric	Product	Limit
OSPF ECMP—maximum number of equal cost multipath OSPF.	BlackDiamond 8800 series (configurable)	2, 4, or 8
	BlackDiamond 10808	8
	BlackDiamond 12800 series	8
	Summit X250e (configurable)	2, 4, or 8
	Summit X450 (configurable)	2, 4, or 8
OSPF external routes—recommended maximum number of external routes contained in an OSPF LSDB without too many other types of OSPF routes.	BlackDiamond 8800 series	20,000
	BlackDiamond 10808	130,000
	BlackDiamond 12800 series	130,000
	Summit X250e	5,000
	Summit X450	5,000
OSPF inter- or intra-area routes—recommended maximum number of inter- or intra-area routes contained in an OSPF LSDB without too many other types of OSPF routes, with one ABR in OSPF domain.	BlackDiamond 8800 series	7,000
	BlackDiamond 10808	7,000
	BlackDiamond 12800 series	7,000
	Summit X250e	2,000
	Summit X450	2,000
OSPF routers in a single area—recommended maximum number of routers in a single OSPF area.	BlackDiamond 8800 series	100
	BlackDiamond 10808	200
	BlackDiamond 12800 series	100
	Summit X250e	50
	Summit X450	50
OSPF subnets on a single router—recommended maximum number of OSPF routed subnets on a switch.	All platforms	400
OSPF virtual links—maximum number of supported OSPF virtual links.	All platforms	32
OSPFv3 areas—as an ABR, the maximum number of supported OSPFv3 areas.	All platforms	16
OSPFv3 interfaces—maximum number of OSPFv3 interfaces.	BlackDiamond 8800 series	256
	BlackDiamond 10808	384
	BlackDiamond 12800 series	256
	Summit X450	128
OSPFv3 neighbors—maximum number of OSPFv3 neighbors.	BlackDiamond 8800 series	64
	BlackDiamond 10808	128
	BlackDiamond 12800 series	128
	Summit X450	64
OSPFv3 virtual links—maximum number of OSPFv3 virtual links supported.	All platforms	16
OSPFv3 external routes—recommended maximum number of external routes.	BlackDiamond 8800 series	10,000
	BlackDiamond 10808	60,000
	BlackDiamond 12800 series	50,000
	Summit X450	10,000

Metric	Product	Limit
OSPFv3 inter- or intra-area routes—recommended maximum number of inter- or intra-area routes.	BlackDiamond 8800 series	6,000
	BlackDiamond 10808	6,000
	BlackDiamond 12800 series	6,000
	Summit X450	3,000
Route policies—suggested maximum number of lines in a route policy file.	All platforms	10,000
RIP-learned routes—maximum number of RIP routes supported without aggregation.	BlackDiamond 8800 series	10,000
	BlackDiamond 10808	10,000
	Summit X250e	3,000
	Summit X450	3,000
RIP interfaces on a single router—recommended maximum number of RIP routed interfaces on a switch.	BlackDiamond 8800 series	256
	BlackDiamond 10808	384
	Summit X250e	128
	Summit X450	128
RIPng learned routes—maximum number of RIPng routes.	BlackDiamond 8800 series	3,000
	BlackDiamond 10808	5,000
	BlackDiamond 12800 series	5,000
	Summit X250e	1,500
	Summit X450	1,500
RSVP-TE interfaces—maximum number of interfaces.	BlackDiamond 10808	
	active	512
	inactive	4,094
	BlackDiamond 12800 R-series	
	active	512
	inactive	4,094
RSVP-TE neighbors—maximum number of neighbors per interface.	BlackDiamond 10808	400
	BlackDiamond 12800 R-series	400
RSVP-TE ingress LSPs—maximum number of ingress LSPs.	BlackDiamond 10808	2,000
	BlackDiamond 12800 R-series	2,000
RSVP-TE egress LSPs—maximum number of egress LSPs.	BlackDiamond 10808	4,000
	BlackDiamond 12800 R-series	3,000
RSVP-TE transit LSPs—maximum number of transit LSPs.	BlackDiamond 10808	2,000
	BlackDiamond 12800 R-series	1,500
RSVP-TE paths—maximum number of paths.	BlackDiamond 10808	1,000
	BlackDiamond 12800 R-series	1,000
RSVP-TE profiles—maximum number of profiles.	BlackDiamond 10808	1,000
	BlackDiamond 12800 R-series	1,000
RSVP-TE EROs—maximum number of EROs per path.	BlackDiamond 10808	64
	BlackDiamond 12800 R-series	64
Spanning Tree (maximum STPDs)—maximum number of Spanning Tree Domains on port mode EMISTP.	All platforms	64
Spanning Tree PVST—maximum number of port mode PVST domains.	All platforms	128

Metric	Product	Limit
Spanning Tree—maximum number of multiple spanning tree instances (MSTI) domains.	All platforms	64
Spanning Tree—maximum number of VLANs per MSTI.	All platforms	500
Spanning Tree—maximum number of VLANs on all MSTP instances.	All platforms	1,000
Spanning Tree (802.1d domains)—maximum number of 802.1d domains per port.	All platforms	1
Spanning Tree (number of ports)—maximum number of ports including all Spanning Tree domains.	All platforms	2,048
Spanning Tree (maximum VLANs)—maximum number of STP protected VLANs.	dot1d dot1w	560 560
SSH (number of sessions)—maximum number of simultaneous SSH sessions.	All platforms	8
Static MAC FDB entries—maximum number of permanent MAC entries configured into the FDB.	All platforms	1,024
Static MAC multicast FDB entries—maximum number of permanent multicast MAC entries configured into the FDB.	BlackDiamond 8800 series Summit X150 Summit X250a Summit X250e Summit X450 Summit X450e Summit X450a BlackDiamond 8810 a-series BlackDiamond 8810 e-series BlackDiamond 10808 BlackDiamond 12800 series	256 1,024 1,024 1,024 256 1,024 1,024 65,000 65,000 65,000 65,000
Static multicast routes—maximum number of static multicast routes.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit X250e Summit X450	256 256 256 128 128
Syslog servers—maximum number of simultaneous syslog servers that are supported.	All platforms	4
TCAM entries—amount of entries available in the lookup tables for Longest Prefix Match routing lookups, learned MAC address, and ACLs.	BlackDiamond 10808, MSM-1 BlackDiamond 10808, MSM-1XL BlackDiamond 12800 series BlackDiamond 12800 R-series	128,000 256,000 49,000 229,000
Telnet (number of sessions)—maximum number of simultaneous Telnet sessions.	All platforms	8
Virtual routers—number of user virtual routers that can be created on a switch.	BlackDiamond 10808 BlackDiamond 12800 series Summit X250e Summit X450	8 8 Not supported Not supported
VLANs—includes all VLANs.	All platforms	4,094

Metric	Product	Limit
VLANs—maximum number of ports.	BlackDiamond 12804	50,029
VLANs (Layer 2)—maximum number of Layer 2 VLANs.	All platforms	4,094
VLANs (Layer 3)—maximum number of Layer 3 VLANs.	All platforms	512
VLANs (maximum active port-based)—number of simultaneously active port-based VLANs.	All platforms	4,094
VLANs (maximum active protocol-sensitive filters)—number of simultaneously active protocol filters in the switch.	All platforms	15
vMAN (maximum ACL rules for vMAN)—maximum number of ACL rules for vMAN.	BlackDiamond 10808 BlackDiamond 12800 series	4,000 4,000
VPLS VPNs—maximum number of VPLS virtual private networks per switch.	BlackDiamond 10808 BlackDiamond 12800 series	500 point-to-point 500 point-to-point
VPLS peers—maximum number of VPLS peers per switch.	BlackDiamond 10808 BlackDiamond 12800 series	16 16
VPLS pseudo wires—maximum number of VPLS pseudo wires per switch.	BlackDiamond 10808 BlackDiamond 12800 series	1000 500
VPLS MAC addresses learned on VPLS pseudo wires—maximum number of MAC addresses learned on VPLS pseudo wires per switch.	BlackDiamond 10808 BlackDiamond 12800 series	100,000 60,000
VRRP (maximum instances)—maximum number of VRRP supported VLANs for a single switch.	All platforms	128
VRRP (maximum VRID)—maximum number of unique VRID numbers per switch.	All platforms	7
VRRP (maximum VRIDs per VLAN)—maximum number of VRIDs per VLAN.	All platforms	7
VRRP (maximum ping tracks)—maximum number of ping tracks per VLAN.	All platforms	8
VRRP (maximum ping tracks)—maximum number of ping tracks per VRRP Instance under 128 VRRP instances. Hello interval: 100 milliseconds Frequency: 3 seconds Miss: 3	All platforms	2
VRRP (maximum ping tracks)—maximum number of ping tracks per VRRP Instance under 128 VRRP instances. Hello interval: 1 second Frequency: 3 seconds Miss: 3	All platforms	4
VRRP (maximum iproute tracks)—maximum number of iproute tracks per VLAN.	All platforms	8
VRRP—maximum number of VLAN tracks per VLAN.	All platforms	8

a. The table shows the total available; see the note included in PD3-77983510.

b. An ACL mask defines a unique match criteria and relative rule precedence. Masks are automatically generated based on the contents of an access-list policy. Only adjacent rules within the policy that have identical match criteria will utilize the same ACL mask. For this reason, it is advantageous to list all rules with the same match criteria together unless a relative precedence with other policy rules is required. Using VLAN-based or wildcard ACLs requires the ACL masks to be allocated on every port in the system.

c. On a BlackDiamond 8810 or Summit X450, it is not advised to have greater than 25,000 total IP routes. Adverse effects can occur with routing tables larger than this, especially when a single network event or CLI command affects a significant number of routes. For example, just after such a network event, the added system load will cause a "save configuration" command to time out.

d. Effective capacity varies based on actual IP addresses and hash algorithm selected.

4 Clarifications and Known Behaviors

This chapter describes items needing further clarification and behaviors that might not be intuitive. The numbers shown in column one of the following tables are for internal reference and can be ignored.

This chapter contains the following section:

- Clarifications and Known Behaviors on page 77
- Issues Resolved in ExtremeXOS 12.0.2.25 on page 107
- Issues Resolved in ExtremeXOS 12.0.2.18 on page 107
- Issues Resolved in ExtremeXOS 12.0.1.11 on page 110

Clarifications and Known Behaviors

Following are the clarifications and known behaviors for supported features in ExtremeXOS 12.0. They are organized into the following sections:

Table 32: General and Platform-Specific PDs

PD Number	Description
General	
PD3-187230035	**"show ports stack-ports rxerrors" Command Shows Wrong Value in RX Over Column** The `show ports stack-ports rxerrors` command output is showing negative and decreasing values in the RX Over column.
PD3-183760131	**IP Directed Broadcast Packets are not Properly Forwarded** IP directed broadcast packets are not forwarded properly using a multinetting configuration.
PD3-186943731	**extremePowerSupplyStatus Object Causes Signal 11 Error** Running an SNMP query for the object extremePowerSupplyStatus results in a process devmgr signal 11 error.
PD3-182634820	**THTTPD Process Cannot be Restarted Using the "start process" or "restart process" Commands** In ExtremeXOS 12.0.1.11, the thttpd process cannot be restarted using the `start process` or `restart process` commands after the process crashes preceded by a "Thread thttpd ID does not respond" log message.
PD3-182546373	**THTTPD Process Gets Stuck in a Loop** The thttpd process gets stuck in a loop, which is causing it to fail to send Hello messages to the Extreme Policy Manager (EPM). As a result, EPM detects that thttpd is stuck and kills the process with a signal 11 error. Once the process is killed by EPM, the process is removed from the system and cannot be restarted using the `start process` or `restart process` commands.
PD3-180718721	**Booting a Dual MSM System May Generate an Error Message**

Table 32: General and Platform-Specific PDs (Continued)

PD Number	Description

	When booting a dual MSM system, the following error message may be displayed in the log for MSM A and MSM B. This error message only applies to MSM B:
	On MSM A:
	`* BD-12804.3 # show log severity error`
	`11/07/2007 20:54:24.34 <Erro:DM.Error> MSM-B: Other MSM is 9 ??`
	On MSM B:
	`BD-12804.1 > show log severity error`
	`11/07/2007 20:54:24.34 <Erro:DM.Error> MSM-B: Other MSM is 9 ??`

PD3-181854281	**Speed and Duplex Settings are Incorrect for 10/100/1000BASE-T GBIC** When changing the configured speed for the 10/100/1000BASE-T copper GBIC, the speed and duplex setting reported in the `show ports` command output is incorrect. The reported values do not reflect the actual speed and duplex setting. This reporting error does not affect the operation of the GBIC.
PD3-149530611	**Switch Experiences Unexpected Reboots** A switch configured with console logging enabled experiences unexpected reboots as a result of an EMS server being killed by EPM.
PD3-132775269	**Telnet Sessions Between Two Switches Causing Mount/Remount Problem** Telnet sessions between two switches using two windows causes one session to hang if both sessions are edited and but only one session is saved.
PD3-77427318	**Do not Use the "configure sys-recovery-level none" Command** The `configure sys-recovery-level none` command can cause the system to behave incorrectly after a process failure. Use this command in this mode only if working directly with Extreme technical support.

PD3-77236982	**Do Not Configure System Recovery Levels "None" and "Switch Shutdown" Together**
	System recovery does not occur when configuring `sys-recovery-level none` in the software and `shutdown` in the hardware on Summit X450a and Summit X450e switches. For example, if you configure the following conflicting commands:
	`configure sys-recovery-level none`
	`configure sys-recovery-level switch shutdown`
	The switch does not shutdown when a hardware error occurs.

PD3-40858541	**10 Gigabit Port Shows Local Fault and Link Down in Syslog When Rebooting** When booting up an I/O module, the switch consistently logs a local fault and link down error in the syslog for 10 gigabit ports.
PD3-29034131	**Saving an SSL Configuration** Saving an SSL configuration causes temporary high CPU utilization.
BlackDiamond 8800 Series of Switches	
PD3-169644346	**Disabling and Enabling a G48T Generates a Log Error** The following log message is displayed when a G48Tmodule is disabled and enabled, or is removed and reinserted: `<Erro:HAL.Card.Error> MSM-A: Anomaly to CPU QOS filter is installed already on ports 1:13 & 1:1`
PD3-151784861	**10G4Ca Modules may Require Custom Pre-Emphasis Settings**

Table 32: General and Platform-Specific PDs (Continued)

PD Number	Description
	10G4Ca modules on BlackDiamond 8800 platforms may require custom pre-emphasis settings on an interface by interface basis as some vendor cables and end devices require custom settings to operate without CRC errors.
PD3-77979043	**Removing the Primary MSM to Initiate Failover Causes Error Messages to Appear in the Log** If you have a mix of BlackDiamond 8800 original, a-series, and e-series modules installed and remove the primary MSM to initiate a failover, informational messages similar to the following appear twice in the log: `<Info:HAL.Card.Info> MSM-B: Module in slot 5 is removed` Since you removed the primary MSM only once, you should see this message once, not twice.
PD3-29694962	**Untagged VLAN Should Drop Packets** On a BlackDiamond 8810 switch, configure one ESRP domain on VLAN1 and VLAN2 respectively. Disable ESRP on VLAN1, and enable ESRP on VLAN2. On VLAN1, send IP packets with the destination MAC being ESRP virtual MAC. Some packets are forwarded by the CPU.
BlackDiamond 10808 Switch	
PD3-175604157	**Dual Speed Copper/Fiber SFP Shows Link as Active When No Cable is Connected** A BlackDiamond 10808 switch with a dual speed copper/fiber SFP shows a link as active even though a cable is not connected.

PD3-124124316	**Unicast Routes with ECMP Enabled Causes Log Errors**
	The following error messages are shown in the log when running 50,000 unicast routes with ECMP enabled:
	`02/05/2007 15:38:37.89 <Warn:HAL.Sys.Warning> MSM-A: hal: Reached maximum otp index allocation`
	`02/05/2007 15:38:37.56 <Warn:HAL.Sys.Warning> MSM-A: Previous message repeated 999 additional times in the last 1 second(s)`

PD3-26882378	**Unsupported Compact Flash Modules May Cause Sluggish Performance** Inserting certain vendors compact flash modules into an external compact flash slot on a BlackDiamond 10808 may result in a system failure.
PD3-68165111	**System Health Check Parity Walk Verification Function Should be Enabled** Various memory locations that are part of the forwarding and routing tables are parity protected on BlackDiamond 10808 switches. The functionality should be turned on so that faults are detectable.

PD3-41204902	**Output for the "show platform ipv4mc group <group address>" Command Contains an "invalid" Entry**
	The output for the `show platform ipv4Mc group <group address>` command contains an "invalid" entry.
	`BD-10808.61 # show platform ipv4Mc g 239.255.255.1`
	`Total Entries:27`
	`Index Type VrId Port Source Group PTI Vlan`
	`004A6 -> 03E3A [3] - invalid`

PD3-63362121	**BlackDiamond 10808 Crashes When Removing a Virtual Router** If you enable SSH, create a virtual router, enable SSH on the virtual router, and then remove the virtual router on a BlackDiamond 10808 switch, the switch may crash. **Workaround:** Remove all services associated with the virtual router, such as OSPF, BGP, PIM, RIP, and so on, before removing the virtual router.

Table 32: General and Platform-Specific PDs (Continued)

PD Number	Description
PD3-61839151	**10G Port Utilization is Incorrect** When you run the `show port utilization` command on a BlackDiamond 10808, the 10G module displays the wrong value.
PD3-59273325	**I/O Modules Fail Due to a Conduit Ping Timeout** I/O modules on a BlackDiamond 10808 with a total of 24,000 OSPF and BGP routes with data traffic may fail due to conduit ping timeout after an MSM failover.
PD3-47375039	**Incorrect Warning in the Log About the MSM Type** The following warning message is found in the log when configuring an MSM using the incorrect MSM type: `09/17/2005 15:41:34.94 <Warn:DM.Warning> MSM-B: MSM-A is of type MSM-1XL which is not checkpoint compatible with MSM-B`
PD3-46512388	**BlackDiamond 10808 May Reboot When All PSUs Experience a Brownout** When all active PSUs on a BlackDiamond 10808 experience a brownout from 220 V AC to 110 V AC at the same time, the switch may reboot.
PD3-39759471	**Dual Speed 100FX/1000LX SFP Lights When Inserted Without a Link** Dual speed 100FX/1000LX SFP is not supported on a BlackDiamond 10808 switch, however, dual speed 100FX/1000LX SFP should not light when inserted without a link.
PD3-41080591	**Intel LR XENPAK Module is not Displaying Correctly** The Intel LR XENPAK module is displaying as an SR module on the BlackDiamond 10808 switch.
PD3-36734601	**Opnext ZR XENPAK Module is not Displaying Correctly** The Opnext ZR XENPAK module is displaying as an SR module on the BlackDiamond 10808 switch.
PD3-37075321	**Intel ER and Intel LR XENPAK Modules are not Displaying Correctly** The Intel ER and Intel LR XENPAK modules are displaying as SR modules or unsupported on the BlackDiamond 10808 switch.
PD3-14127903, PD3-13538171	**Egress Mirror Packets are Being Sent to Mirror Port in Link Down State** Mirrored egress packets are being sent to the mirror port even when the port is in the link down state.
PD3-7347167, PD2-199490211	**Shared Portion of the (TCAM) Memory Blocks Cannot be Reclaimed** Once the shared portion is allocated to one resource type, such as an FDB or ACL, it cannot be reclaimed to be used for other resource type entries.
PD3-17230511	**Hot Swapping the Master MSM** Hot swapping the master MSM may generate the following message: `WKNINFO: Invalid self slot number 0`
PD2-238395030	**Overflowed Routes and Entries are not Installed Automatically** When TCAM space becomes available after an overflow situation, the overflowed routes and entries are not installed automatically.
BlackDiamond 12800 Series Switches	
PD3-187808062	**Switch Does not Show Warning Message for Down Revision MSM and I/O Modules** A BlackDiamond 12800 series switch does not show a warning message on the console for down revision MSM and I/O modules after initialization.

Table 32: General and Platform-Specific PDs (Continued)

PD Number	Description
PD3-169776366	**Connecting a BlackDiamond 12800 to a Summit X450 Causes an I/O Module Failure** Connecting a BlackDiamond 12800 series switch with two ports to a Summit X450 and also connecting the BlackDiamond 12800 management port to the Summit X450 port 15 causes an I/O module failure.
PD3-24601141	**802.1P Precedence Support** Incoming 802.1P precedence is not supported when ports are used for vMAN.
PD3-125511903	**System Fails with a Signal 10 Error When Running an MSM Failover** A system failure occurs with a signal 10 error when performing a run msm-failover immediately after the backup MSM is in-sync
PD3-131941899	**Disabling an Enabling a GM-20XT I/O Module puts Slot in Failed State** Disabling and enabling a GM-20XT I/O module twice causes the slot to enter the Failed state and displays the following error message. `Error Generic Error(-1) from HAL on CardExec POWER_OFF(10) for slot 1`
PD3-130441271	**Traffic Queues with Metering are not Applied Correctly** Traffic queues with metering are not applied correctly with large packets, such as 256, 512, and 1,024. The traffic fluctuates between different rates when the packet size is above 200.
PD3-86738591	**Traffic Queue Statistics are Incorrect when Switch is Configured** Traffic queue statistics are incorrect when a BlackDiamond 12800 series switch is configured to work in H-QoS mode. Statistics counters are accurate when the switch is configured in the PRI mode.
PD3-98333969	**Disabling and Enabling a Port Can Take 30 Seconds for Port to Activate** During continuous FDB learning, disabling/enabling a port can take up to 30 seconds for the port to activate.
PD3-56223462	**ESRP Master Change from BlackDiamond 12800 Series to BlackDiamond 8800** Changing the ESRP master from a BlackDiamond 12800 series switch to a BlackDiamond 8800 or Summit X450 causes a traffic loss of more than eight seconds.
PD3-56812371	**Packet Loss Occurs When A BlackDiamond 12800 Series Switch Becomes ESRP Master** When ESRP is running on a BlackDiamond 12800 series switch and a BlackDiamond 8800, there is a three second traffic loss when the BlackDiamond 12800 series switch becomes the master rather than the BlackDiamond 8800.

PD3-62516612	**Backplane Link to Backup MSM Message is not Correct**
	Since the backup MSM does not have access to I/O modules until the backup MSM becomes the master, the entry `B - Backplane link to Backup MSM is also Active` should be deleted from the following message:
	`BD-12804.11 # show slot`
	`Slots Type Configured State Ports Flags`
	`Slot-1 GM-20XT GM-20XT Operational 20 M`
	`Slot-2 GM-20T GM-20T Operational 20 M`
	`MSM-A MSM-5 Operational 0`
	`Flags : M - Backplane link to Master MSM is Active`
	`B - Backplane link to Backup MSM is also Active`

Table 32: General and Platform-Specific PDs (Continued)

PD Number	Description
PD3-62187218	**"show version" Command May Display Old Firmware Versions If Run Between "install firmware" Command and Rebooting System** The `show version` command may display the old firmware version if you run the command between the `install firmware` command and the `reboot` command on a BlackDiamond 12804.
Summit Family of Switches	
PD3-182873571	**Disabling and Enabling a Summit X450 and X450a Series Switches May Cause Port to Stay in the "Ready" State** When a 10/100/1000 copper GBIC is plugged into a Summit X450 or Summit X450a-24X switch, disabling or enabling the port may cause the link to stay in the "ready" state.
PD3-163837787	**Debug Tool "gdb" Not Found** The debug tool "gdb" is not found on the switch; you must install the image `debug.xmod`. For example, for a Summit X450 switch running ExtremeXOS release 12.0.2.18, you must install the `summitX-12.0.2.18-debug.xmod` image.
PD3-182532561	**Summit X450a-24X Switch May not Autonegotiate to 100 Mbps if Switch is Set to the Default Autonegotiation** The Summit X450a-24X switch with a 10/100/1000 copper GBIC may not autonegotiate to 100 Mbps if the switch is set to the default autonegotiation configuration and the link partner speed is set to 10 Mbps or 100 Mbps. The physical layer is correctly configured to 100Mbps, but the speed reported is not correct. **Workaround:** Configure the speed on a Summit X450a-24X to 100 or 10 Mbps (forced or autonegotiation).
PD3-179276997	**"show ports information" and "show ports configuration" commands Show Ports as Available and Enabled** Running the `show ports information` and `show ports configuration` commands on a Summit switch that does not include an XGM2 option card erroneously displays the ports on the card as available and enabled.
PD3-176671740	**Plugging a ZR XENPAK into a XGM2-xn-1 Module is Shown as NONE** When enabling a Summit X450 switch in stacking mode with a ZR XENPAK that is plugged into a XGM2-xn-1 module, the Media Primary column displays NONE in the show ports configuration command output.
PD3-168702411	**Link is Active on One Node and Not Active on the Other When FX is connected with an SX Link** On a Summit X250e-24x, when a link is connected to an SX SFP mini-GBIC on one side and a 100 FX on the other side of the link, the link is shown as being up on the 100 FX side but the link is down on the SX side.
PD3-176482145	**L2 Tunneling Protocol Does not Work on a Summit X450 After Rebooting a vMAN+PVST Configuration** The L2 tunneling protocol using the ACL action `replace-ethernet-destination-address` does not work on a Summit X450 after rebooting a vMAN+PVST configuration.
PD3-131375426	**Autopolarity does not Work on Combo Ports** Configuring autopolarity does not work on the combo ports on the Summit family of switches.
PD3-137352385	**Software Upgrade on Summit X250e Results in Upgrade Failure** When you configure 2,500 or more VLANs in the DUT and upgrade a Summit X250e to a later version of software, the DUT crashes and reboots continuously, resulting in an upgrade failure.

Table 32: General and Platform-Specific PDs (Continued)

PD Number	Description
PD3-141468131	**LED Does not Light for Loopback Ports When Enabling the One-to-Many Mirroring** For Summit X450-24t platforms, the LED does not light for loopback ports when enabling one-to-many mirroring. This is an LED-specific issue; mirroring is not affected.

PD3-7894731	**Port Number Display is Misleading in Messages**
	Some error and warning messages display a misleading port number. For example, if you configure a duplicate receiver port on the MVR VLAN mc4, using the following command:
	`configure mvr mc4 add receiver port 1`
	`You will see the following error message:`
	`MVR receiver port 256:2 already configured on Vlan mc4`

PD3-77978516	**L3 Algorithm Flags can be Ignored in the "show ports sharing" Command Output** On the Summit X450a and X450e series switches, you can ignore the "L3" algorithm flags displayed in the `show ports sharing` command output. These switches currently support the Layer-2 and Layer-3/Layer-4 combination algorithms.
PD3-75224031	**Reconfiguring the vMAN Ethernet Type is not Effective Until Shared Port is Deleted and Added** Reconfiguring the vMAN ethertype value from 0x8100 to a value other than 0x8100 will not become effective until disconnecting and adding back the port being shared by the vMAN and VLAN. This means the EtherType value remains 0x8100 even though the `show vMAN etherType` command shows the re-configured value.
PD3-77711011	**"Slot" Should not be Included in "show inline-power stats" Command Output** The word "slot" should not be included in the output of the `show inline-power stats` command.
PD3-77711042	**Priority Column Should not be Included in "show inline-power configuration" Command Output** The Priority column should not display in the output of the `show inline-power configuration` CLI command when running the command on a Summit X450-24p PoE switch.

PD3-43606168	**"show log" Command Output Filled with sFlow Receiver Missing Message**
	If sFlow does not have a collector configured using the `configure sflow collector` command, the `show log` command generates the following messages:
	`08/23/2005 12:28:09.55 <Noti:sflow.debug.AddCntSmplFail> : Could not add the counter sample for port 0:1020, as receiver is not configured.`
	`08/23/2005 12:07:49.55 <Noti:sflow.debug.AddCntSmplFail> : Previous message repeated 61 additional times in the last 1200 second(s).`

PD3-40266236, PD3-40233121	**Redundant Ports not Correctly Moving to Other Ports in Load Sharing Mode** Traffic on load share ports configured as redundant ports incorrectly moves to other ports in the load share group during link transition.
PD3-34629664, PD3-25415431	**"restart ports" Command Runs Too Quickly on a Summit X450** Connecting a Summit X450 to a BlackDiamond switch and issuing the `restart ports` command from the Summit X450, the Summit X450 log shows that the link was brought DOWN and UP in 0.5sec, but the BlackDiamond switch does not see the link UP/DOWN state.
PD3-34629550, PD3-19190526	**Flow Control is Always Reported for 1000 Mbps Link Speed**

Table 32: General and Platform-Specific PDs (Continued)

PD Number	Description
	When a Summit X450 is connected to a Summit 400, the `show ports configuration` command on the Summit X450 always reports SYM as flow control.

Table 33: Feature-Specific PDs

PD Number	Description
ACL	
PD3-135200936	**ACL Policy File is Applied to a Port even though the Associated Meters are not Created** When an ACL policy file containing meters associated with ACL rules is applied to a port, the system should verify that the meters are present before installing the ACL policy file. If meters are not present, the system should generate an appropriate error message and the ACL policy file should not be installed.
PD3-127190211	**VLAN ACLs do not Work When vMAN Ethertype is Set to 0x8100** VLAN ACLs do not work when a vMAN EtherType is set to 0x8100. Incoming traffic is not matched against the rules in the ACL policy file and the traffic is forwarded without applying the matched rule in the policy file.
PD3-135380560, PD3-134870425	**Installing/Uninstalling ACL Rules with Meters may take a Long Time** For Summit X450 and BlackDiamond 8800 switches, installing, unconfiguring, and refreshing a large number of static or dynamic ACL rules with meters may take a long time. **Workaround:** Install ACL rules with meters in the order "higher precedence first," and uninstall ACL rules with meters in the order of "lower precedence first."
PD3-118223441, PD3-57946832, PD3-26612201, PD3-24794592	**Before Changing a VLAN Tag, Unconfigure all ACLs Applied to the VLAN** Before changing a VLAN tag, make sure you unconfigure all the ACLs applied to the VLAN. Also, after changing the tag, reconfigure the ACLs to be applied on the VLAN.
PD3-127842058, PD3-127842159	**Only Ingress Applied CLEAR-Flow Rules are Triggered** With CLEAR-Flow enabled, only ingress applied CLEAR-Flow rules are triggered.
PD3-126824622	**IPv6 Protocol ICMP Should not be Allowed** If an IPv6 address is included in a configuration, use ICMPv6 for the protocol. ICMP (IPv4) should not be allowed.
PD3-121018177	**Redirect-Port is not Supported on Egress Ports** Action redirect-port is not supported on egress ports. Even if redirect is applied to an egress port, while redirect-port has no effect on egress traffic, the counter should work correctly.
PD3-100694069	**Scaling Dynamic ACLs Generates Log Messages**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description

	Scaling dynamic ACLs on BlackDiamond 10808 and BlackDiamond 12804 switches when approximately 2,000 rules are created and configured to an interface (VLAN, port, or any), displays the following log message:
	`* BD-10808.2 # show log...`
	`10/11/2006 15:16:12.04 <Info:EPM.cpu> MSM-A: CPU utilization monitor: process hal consumes 99 % CPU...`
	This also occurs when running the `save configuration` and `reboot` commands when the switches reboot.

PD3-117123801, PD3-94304671	**ACL IGMP Counters are Counting Twice the Actual Transmitted Packets** Egress ACL counters for the slow-path forwarded IP packets are counting twice the actual packets. Slow-path forwarded IP packets are IGMP, IP packets with IP options, and IP packets showing the address that is not resolved.
PD3-88458683	**Default Egress Deny-All ACL Does not Block Multicast Traffic** If you run the `clear ipmc fdb` command, initially some multicast packets are forwarded in slowpath. Those slowpath forwarded multicast packets are being denied by ACL.
PD3-123322724	**CLI Does not Show Error when Mask is Given for Ethernet Destination Address** The CLI does not show any error messages when a mask for an Ethernet destination address is given in a policy file without using the mask keyword.
PD3-120701781	**ACL VLAN Translation does not Work Properly on vMAN Ingress Port** Applying a VLAN translation ACL does not work properly and traffic is forwarded with the same inner tag, but the counter is shown as incrementing.
PD3-76416480	**ACL Cannot Deny vMAN Traffic with Unknown Destination Address** When an egress ACL is used to deny vMAN traffic with unknown unicast, multicast, and broadcast destination addresses, the egress ACL cannot deny the traffic.
PD3-94304401, PD3-42872248	**Creating Dynamic ACLs Using Operands Results in an Error** Creating dynamic ACLs using the operands "<" or "<=" results in an error. Use "lt" and "lte" instead.

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
PD3-77983510	**Summit X450a and Summit X450e series switches and BlackDiamond 8800 a-series and e-series Modules: Boot Time and Timing for Applying ACLs** Summit X450a and Summit X450e series switches and BlackDiamond 8800 a-series and e-series modules provide more powerful ACL capabilities. Because of this, the amount and complexity of ACL rules will naturally impact the time needed to process and apply the ACL rules to the switch. This will also impact switch bootup time. Access Control List limitations fall into two areas: physical and virtual. Physical Limits—Summit X450a and Summit X450e series switches: The per-VLAN, wildcard (port any), and single-port access list installation limitations are 1024 rules for the Summit X450e and 2048 rules for the Summit X450a. Physical Limits—BlackDiamond 8800 a-series and e-series modules: The per-VLAN, wildcard (port any), and single-port access list installation limitations are 1024 rules for the e-series modules, and 2048 rules for the a-series modules. Extreme Networks recommends that you configure ACLs as per-VLAN, wildcard, or single-port. If either of the following is true, you will have to configure ACLs with multi-port lists: Your application requires that ports do not have a homogeneous ACL policy. When BlackDiamond 8800 original series modules are operational in the same chassis, it may be necessary to configure ACLs to specific port-lists instead of as wildcard or per-VLAN. This is because the original series modules have smaller physical limits. Virtual Limits—Summit X450a and Summit X450e series switches: When configuring a multi-port ACL, use the following guideline. The total ACL count (as calculated by ACL rules times ports applied to) should not exceed 48,000 total ACL rules. For example, applying a 1,000 rule policy file to a 48 port multi-port list is supported (1,000 rules * 48 ports in the list <= 48,000). Virtual Limits—BlackDiamond 8800 a-series and e-series modules: When configuring a multi-port ACL, use the following guideline. For any a-series or e-series blade in the system, its total ACL count (as calculated by ACL rules times ports applied to) should not exceed 48,000 total ACL rules. For example, applying a 1,000 rule policy file to a 48 port multi-port list on an a-series module on slot 1 and an e-series module in slot 2 is fine. Neither module exceeds the 48,000 total ACL rules. Excessive boot times and CPU resource starvation can be seen with larger total rule counts. If your application requires additional capacity, contact Extreme Networks.
PD3-56605924	**Only One Egress ACL per vMAN Currently Supported** Multiple egress vMAN ACL rules with identical IF-conditions but different egress ports cannot be distinguished. Packets are going to be forwarded based on only one of the applicable rules.
PD3-56552466	**Changing the Name of a Rule but not its Conditions or Actions Causes an Error** Changing the name of a rule in an ACL policy but not its conditions or actions, and then performing a refresh, causes a "duplicate" error on BlackDiamond 8806, BlackDiamond 8810, and Summit X450 switches.
PD3-58200199, PD3-42447111	**ACL actions mirror-cpu and log/log-raw not logging messages** The ACL action mirror-cpu and log do not work.

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
PD3-54549831	**Policy-Based Redirect Cannot Redirect Across Two Virtual Routers** Policy-based redirect works properly within one virtual router (tagged or untagged VLANs), however, if you try to redirect traffic to a VLAN that belongs to a virtual router other than the one sending ingress traffic, the redirect does not work.
PD3-55929951, PD3-41829516	**ACL ICMP Keyword for Timestamp is not Working** The keyword `icmp-type timestamp` when used in an ACL policy match condition does not work. Using the ICMP number code instead of the keyword works correctly (icmp-type 13).
PD3-51329744	**Modifying a Port Range in an ACL Rule May Cause an ACL Blackhole** Modifying the port range of an ACL rule may cause a temporary blackhole or packet leak while refreshing on a BlackDiamond 8806, BlackDiamond 8810, or Summit X450 switch. To avoid this, modify the port range ensuring the new range does not overlap the old range. Alternatively, to avoid the packet leak, enable blackholing.
PD3-27536111	**Cannot Save Policy File Using a Different Name** When you edit tcpDestPort.pol using the VI editor and save it with a different filename, the new file is not applied.
PD3-28320337	**MAC and IP MAC Entries Allowed in the Same IPv6 ACL Rule Entry** MAC and IP MAC entries are being allowed in the same IPv6 ACL rule entry. L2 and L3/L4 rules should not be allowed in one entry; this should fail the grammar check but does not.
PD3-28320363	**Invalid Encapsulate Value for IPv6** In IPv6, the encapsulate value is "next header," which is not currently a valid attribute.
BGP	
PD3-41952658	**Peer IP Address is Missing in BGP Traps** BGP traps transmitted from a BlackDiamond or Summit X450 switch are missing the peer IP addresses.
CLEAR-Flow	
PD3-95652911, PD3-95652994	**"show clear-flow vlan" Command Displays Invalid Threshold Type** When using the `show clear-flow` command, RL is not included in the Threshold Type with CN, DT, and DR.
PD3-60258721	**CLEAR-Flow is Not Supported on Summit X450 and BlackDiamond 8800** CLEAR-Flow is not supported on Summit X450 and BlackDiamond 8800 switches.
PD3-71744964, PD3-57208227	**CLEAR-Flow Does not Require a Space around Operators** CLEAR-Flow does not mandate a space around operators. This should be required.
PD3-16311713	**CLEAR-Flow is only supported on BlackDiamond 10808 and BlackDiamond 12804 Switches** A syntax error is not displayed when a policy file is configured using CLEAR-Flow rules on BlackDiamond 8810, BlackDiamond 8806, and Summit X450 switches. The rule is silently ignored.
CLI	
PD3-125018491	**Load Script Unable to Process Banner Configuration** The `load script` command is unable to process banner configuration.

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
PD3-77316227	**"show configuration" Command Output Includes Invalid Switch Prompt** The `show configuration` command output includes the invalid switch prompt `configure vr VR-Default add ports 1:1-2:48, 4:1-10:48`.
PD3-71725881	**Timezone/DST Name Truncates at Seven Characters** When configuring an optional name for the timezone/DST on the Summit X450 family of switches, the timezone name truncates at seven characters. The system default is six characters.
PD3-57182431	**RX Align Counter is not Incremented** For the incoming traffic with alignment errors, the "RX Align" counter in the output of the `show ports <port number> rxerrors` command is not incremented. Instead the "RX CRC" counter is incremented.
PD3-63858286	**"upload configuration" Command Contains RIP Configuration Commands** The `upload configuration` CLI command contains RIP configuration commands in spite of there not being a RIP VLAN.
PD3-63772664, PD3-63875328, PD3-63858254, PD3-63858238	**"upload configuration" Command Generating Invalid CLI** While uploading a configuration using the `upload configuration` command, the following invalid CLI commands appear. These commands are harmless: On a Summit X450 switch: • `configure slot 1 module SummitX450-24t` (PD3-63772664) • `configure mstp region 00049620ad93 create stpd s0` (PD3-63875328) • `configure ospf vlan com` (PD3-63858254) • `configure firmware` (PD3-63858238)
PD3-40450253	**"show ports mgmt utilization" CLI Command Does not Show any Statistics** The `show ports management utilization` command does not show any statistics. The command output is all zeros.
Control Protocols	
PD3-160517465	**EAPS Topology Change Cannot Flush FDB Entry** Configuring EAPS and MSTP on the same port for the same VLAN results in a longer convergence time for the EAPS topology change. Even after a RxPduRingUpFlush is triggered for the topology change, the FDB entry is cleared.
PD3-125288233	**MSTP Fails to Converge when Ethernet Type is 0x8100** MSTP fails to converge when a vMAN Ethernet type is set to 0x8100 on a BlackDiamond 12800 series switch.
PD3-94406464	**When a Port Link is Down or Disabled, UPM Should Register a Device-Undetect** When an LLDP enabled port link is down or disabled, Universal Port Manager may take up to 30 seconds to register a UPM device-undetected event.
PD3-79194922	**Convergence Time May Increase After Removing Root Bridge from dot1s Network** Convergence time may increase (approximately 90 seconds) when a root bridge is removed from a dot1s network.
PD3-75421071	**CIST Ports Link-Type Configured as Point-to-Point Lost When Configuration is Uploaded and Downloaded**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
	When creating a CIST domain and then configuring the link-type as point-to-point for CIST, the link-type configuration is lost when the uploaded configuration is downloaded.
PD3-77283998	**Summit X450a May Briefly Lose Data During a Failover** Large routing table updates affect the convergence time for EAPS and VRRP failovers.
PD3-67713552	**MSM Failover on ESRP Slave Running IGMP Causes Packet Loss** When a BlackDiamond 8800 is an ESRP slave and you issue the run failover command, it will send IGMP reports with the ESRP VMAC address, which results in MAC relearning and an initial packet drop for approximately 10 seconds.
PD3-60905520	**STP Blocks CFM Packets** Connectivity Fault Management (CFM) packets are not received on ports blocked by STP, EAPS, and ESRP.
Device Management	
PD3-160309254	**Configuring and Using SNTP Date Correction** The last paragraph of step 2 in the section titled "Configuring and Using SNTP" in the *ExtremeXOS Concepts Guide* should read: "By default beginning in 2007, Daylight Saving Time is assumed to begin on the second Sunday in March at 2:00 AM, and end the first Sunday in November at 2:00 AM and to be offset from standard time by one hour. If this is the case in your time zone, you can set up automatic daylight saving adjustment with the command." This correction will be included in the *ExtremeXOS Concepts Guide, Software Version 12.1*.
PD3-125671355	**System does not Display Log Message when Running Diagnostics on Backup MSM** The device manager does not log a message stating that diagnostics are being run on the backup MSM, or that diagnostics are complete. For example: `02/14/2007 12:51:30.06 <Noti:DM.Notice> MSM-B: Slot-1 running diagnostics`
PD3-126243853	**HTTPS with Key Length of 4,096 has High CPU Utilization** Using a key length of 4,096 in an SSL certificate causes high CPU utilization during HTTPS sessions.
PD3-84049005	**DOS Console Window Does not Wait for User Input** The DOS console window does not wait for user input after executing the unconfigure switch all command.

PD3-42934079	**CX4/LX4 XENPAK Port Must be a Tagged Port on a BlackDiamond 10808**
	When adding a CX4/LX4 XENPAK port to a VLAN on a BlackDiamond 10808, it must be added as a tagged port or the following error message is generated:
	`BD-10808.32 # config cx4 add port 5:3`
	`Error: 5:3 must be added as tagged port to a vlan on this revision of IO module`
	`Configuration failed on backup MSM, command execution aborted!`

PD3-77949095	**"show configuration" Command Output Shows Wrong Information** The output for the `show configuration` command includes some default configuration commands that are not available for user configuration.
PD3-50854648, PD3-40438530, PD2-232334464	**No Warning When Deleting User VR from Another User VR**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
	A warning message is not displayed when deleting a user virtual router from another user virtual router.
PD3-30209032	**"show configuration vlan" Command Shows an Invalid Command** A configuration port display-string and an invalid command are displayed in the show configuration vlan command.
PD3-12654351	**Configuration Error After Deleting IP on Virtual Router Used by a RADIUS Server** If you configure a RADIUS server to point to an IP address that is found off of the default virtual router, unconfigure the IP address on the default virtual router, and reboot the switch, the following error message is generated: `Error while loading structure <radiusAuthServer><server_no>1</server_no><encrypted_secret/><bad_authenticators>0</bad_authenticators><vr><![CDATA[VR-Default]]></vr><access_rejects>0</access_rejects><access_accepts>0</access_accepts><host_ipaddr>10.66.200.10</host_ipaddr><radiusAuthClientPendingRequests>0</radiusAuthClientPendingRequests><access_challenges>0</access_challenges><client_timeouts>0</client_timeouts><radiusAuthClientPacketsDropped>0</radiusAuthClientPacketsDropped><hostname/><radiusAuthClientMalformedAccessResponses>0</radiusAuthClientMalformedAccessResponses><unknown_types>0</unknown_types><rtt>0</rtt><client_ipaddr>10.5.3.84</client_ipaddr><`
Diagnostics	
PD3-74554921	**sys-health-check Configurations are not Stored in Uploaded Configurations** System health check related configurations are not stored in uploaded configurations.
Documentation	
PD3-162802718	**Merit RADIUS Server is not Supported** Extreme Networks does not currently support the Merit RADIUS server.
PD3-157660649	**Network Login Command Corrections** The following corrections will be incorporated into the *ExtremeXOS Concepts Guide, Software Version 12.1*: • A Network Login authenticated entry is cleared by an FDB timeout. This applies to web-based, MAC-based, or 802.1x authentication. • The statement that the logout window refreshes itself at every configured time interval under the `enable netlogin session refresh` command is not correct. The statement "Session refresh is disabled by default" should read "Session refresh is enabled by default." The following correction will be incorporated into the *ExtremeXOS Command Reference Guide, Software Version 12.1*: • The statement "The session refresh is enabled and set to five minutes by default." in the Usage Guidelines for the `disable netlogin session-refresh` command should read "The session refresh is enabled and set to three minutes by default."
PD3-78599376	**"show inline-power info detail" Command** On the Summit X450a, the `show inline-power info detail` command output is different from that shown in the documentation. For this platform only, the priority field is not displayed. Priority only applies to the modular PoE devices.
PD3-78599401	**"show inline-power" Command**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
	On the Summit X450a, the `show inline-power` command output is different from that shown in the documentation. For this platform only, the disconnect precedence and budgeted power fields are not displayed. These only apply to the modular PoE devices.
PD3-131018386	**Root Blocker ID Toggles Between Original and Changed IDs** After changing the root blocker and partner IDs, the displayed root blocker ID toggles between the original and the changed IDs.
PD3-102844558	**Number of EAPS Domains Supported by Advanced Edge License** Although it is possible to configure more than four EAPS domains on a switch with an Advanced Edge license, this is not supported.
PD3-86015166	**Segment Port Warning in Log When Disabling Port Sharing on a EAPSv2 Segment Port** When LACP is enabled on a link between two switches, when disabling port sharing, the following warning is displayed in the log for each of the protected VLANs: `08/02/2006 12:20:31.36 <Warn:EAPS.SharedPort.SegPortWarning> EAPS Shared-port 4, Segment-port 4 - No vPif for vlan pv24`
PD3-86015057	**Critical VLAN Error seen When Disabling Port Sharing on Ring Port** The following error message is displayed in the log when disabling port sharing on ring ports: `08/01/2006 19:49:32.55 <Crit:vlan.err.criticalInfo> Critical Info: handleVMngrProtoIfSetState procName:eaps protolId:0x80 not registered vpif->l2Protos:0x0, vpif:1:4 on pv50 ingress:0x5 egress:0x1 dereg:0 (0 of 50)s`
PD3-96983520	**Changing Shared Port Link ID When the Shared Link is Down** Changing the EAPS shared port link ID of a partner/controller pair while there is a failure in the EAPS network is not recommended and may cause a loop in the network.
PD3-104885349	**Traffic Loss Occurs When a Shared Link Comes Up** When traffic is running between shared links, FDB entries are incorrectly learned on BlackDiamond 10808 and BlackDiamond 12804 switches. Traffic loss occurs until the incorrectly learned FDB entries age out.
PD3-97153785	**If Multiple Shared Links are Down, a Loop is Created** In a specific EAPS topology, if multiple shared links are down, a loop is created.
EAPS	
PD3-78599455	**Number of EAPS Domains Supported by Advanced Edge License** Although it is possible to configure more than four EAPS domains on a switch with an Advanced Edge license, this is not supported.
PD3-135517703, PD3-87003427, PD3-78960443, PD3-78302829	**Simultaneously Disabling Three Shared Port Links can Cause an EAPS Loop** Configurations having three shared links, where the shared link with the lowest ID is in the middle, the root blocker marks the segment as "blocking-down," but the ports are not in a blocked state. To get out of the loop, restore the shared links. To avoid encountering this condition, insure that no more than two shared links become disabled.
PD3-56877301	**Disabling a Slot on a BlackDiamond 12804 Causes a Loop in EAPS Setup** Configuring two EAPS sharing links on a slot and disabling both sharing links at the same time causes a loop of approximately 1.5 seconds on a BlackDiamond 12804.

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
PD3-54870537, PD3-45729158	**EAPS with Load Sharing Enabled/Disabled Causes Control Packets to be Received on Port** Misconfigured EAPS control VLAN ports may not be detected, causing EAPS PDUs to be accepted into the system even though they were received on an incorrect port.
PD3-27767509, PD3-27536496	**EAPS in Active Root Blocker State** When EAPS is in the Active Root Blocker state, that is, there are two more common links that are down, it is possible to have a disconnected network on some VLANs. The VLANs that are affected are the VLANs that do not span the entire network. This happens because EAPS forces blocking of VLANs to prevent a loop. EAPS does not check to see if a loop was going to happen in the first place, thereby causing a disconnected network for those VLANs.
PD3-30112655	**EAPS in Root Blocker State When Multiple Common Links are Down** When multiple shared links are down, a controller may take up to a second to put itself into Root Blocker state. There could be a brief temporary loop during this time (up to a second).
PD3-176462601	**EAPS Takes 120 ms to 160 ms to Recover After Restoring a Link Failure** EAPS takes approximately 120 milliseconds to 160 milliseconds to recover after restoring a link failure.
ESRP	
PD3-61629918	**VLAN Tracking Fails after an MSM Failover** On a BlackDiamond 8810, when an ESRP domain is configured with VLAN tracking, ESRP transitions to the SLAVE state when the tracked VLAN goes down (that is, all the VLANs ports go down). After an MSM failover, the ESRP domain transitions to the master state, even though it still shows the tracked VLAN is down.
PD3-52741820	**Disabling a Shared Port Makes the ESRP Port Restart configuration disappears** Disabling a shared port results in the ESRP port restarting and the configuration disappearing.
PD3-26330059, PD3-14890821	**Potential Problem with Graceful Disable of ESRP** Graceful disable of ESRP may cause a momentary loop in the network.
IP Routing Protocols	
PD3-161152153	**High CPU Utilization Message is Logged for RIP Process** A switch experiences high CPU usage and logs an error message when running a RIP process when an snmpwalk is performed even though RIP is globally disabled: `07/12/2007 19:47:43.10 <Info:EPM.cpu> MSM-A: CPU utilization monitor: process rip consumes 99 % CPU`
PD3-132508261	**MTU Size for a VLAN is not Configured** When issuing the `enable jumbo-frame port all` command on a BlackDiamond 8810, the MTU size for the VLAN is not configured. Sending 5,000 byte traffic works correctly. However, if you disable jumbo-frames on the egress port the error message `Packet too big` is displayed.
PD3-128093864	**MSDP SA Responses from non-RPF Peers are not Processed** MSDP Source-Active responses received from non-RPF peers are not processed.
PD3-100339658	**ICMP Packets are not Answered Correctly** The switch does not answer back IPv6 ICMP packets correctly.

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
PD3-90875982	**IGMP Memberships are Flushed if STP Link Goes Down** When an STP link goes down, IGMP memberships are flushed, resulting in a drop in traffic.
PD3-52605136	**IPv4 Capability Must be Configured for BGP Restart to Work Properly** For BGP graceful restart to work with third party operating systems, IPv4 capability may have to be configured in ExtremeXOS.
PD3-40476272, PD3-28467998	**"show pim" Command Should Return an Error Message When Protocol Not Added to User VR** When a protocol PIM is not added to a user VR, the switch does not return an error message when you run the `show pim` command from the user VR.
IPv6 Unicast	

PD3-139714881	**Info Level Messages in log when Configuring Link Aggregation on VLAN Associated with IPv6 Tunnel**
	The following info level messages appear in the log when link aggregation is configured on a VLAN associated with an IPv6 6-to-4 tunnel:
	`05:01:49.04 <Info:HAL.VLAN.Info> MSM-B: pibIPv6InstallTunneledLinkLocalFilter: Could not install filter unit 12, Entry exists`
	`04/24/2007 05:01:49.05 <Info:HAL.VLAN.Info> MSM-B: pibIPv6InstallTunneledLinkLocalFilter: Repaired filter unit 12`
	These messages do not affect the operation of the switch.

Mirroring	
PD3-79867211	**Mirroring Port Should Not be Allowed in Load Sharing** If you create a load sharing group (trunk), then enable mirroring to a port, the software allows you to add the mirroring port to the load sharing group.
PD3-28378521	**Enabling Load Sharing on a Mirrored Port** Enabling load sharing on a port that is being mirrored causes the mirroring to stop.
MPLS	
PD3-177361681	**Existing MPLS Forwarding Data not Installed on Newly Inserted BlackDiamond 12800 I/O Module** Existing MPLS forwarding data is not installed on newly inserted BlackDiamond 12800 series switches, which can cause problems when receiving and transmitting MPLS packets on those I/O modules. **Workaround:** Disable and enable MPLS.
PD3-139423053	**RSVP-TE: LSP Summary Statistics take Excessive Time to Calculate** Running the `show mpls rsvp-te lsp summary` command on a system configured with 2,000 ingress LSPs takes an excessive amount of time to process.
PD3-135927701	**"show vpls detail' Command Does not Display Updated Counters** The `show vpls detail` command does not display the updated counters (RX Pkt and RX Bytes) when using "q" to quit. The counters are updated after running the complete command.
PD3-121985381	**Packets Larger than Configured Jumbo Frame Size are Forwarded**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
	You cannot configure an IP MTU that is greater than the configured jumbo frame size. However, when the jumbo frame size is configured using a smaller value than the IP MTU, the configuration is accepted and the traffic is forwarded using the larger packet sizes.
PD3-118914021	**Label not Advertised for a Default Route in a Stub Area** When an OSPF neighbor is configured between two LSRs and MPLS, and an LDP session is configured between them, the ABR router advertises a default route to the internal router. The default route is not mapped to a label in the internal router because the ABR does not advertise the label
PD3-97057691	**Mirrored RSVP Path Message Packets have Incorrect IP Header Checksums** When creating a mirrored port and viewing all traffic on a BlackDiamond 10808, the RSVP path packets have incorrect checksums. These path messages occur on egress traffic from the BlackDiamond 10808.
PD3-109748431	**"show tech" Command Shows Erroneous MPLS CLI on a Non-MPLS License System** The `show tech` command shows erroneous MPLS CLI on a non-MPLS license system running on a BlackDiamond 10808. MPLS should determine if the system is MPLS licensed and only then show the CLI.
PD3-133340423	**LDP Adjacency Breaks after Enabling PHP Feature** The PHP feature will not work correctly and may break LDP adjacency with its neighbors. Currently, there is no workaround.
PD3-99318269	**"show mpls rsvp-te lsp detail" Command may not Show Error Condition** If the transmit bandwidth between two RSVP-TE neighbors is sufficient for a given LSP, but the receive bandwidth is not, the LSP does not come up. The reason for the error is not displayed in the `show mpls rsvp-te lsp detail` output.
PD3-92653036	**Egress LSPs using Advertised Implicit NULL Labels are not Displayed** The `show mpls label`, `show mpls rsvp-te label`, and `show mpls rsvp-te lsp` command output currently does not display egress LSPs using advertised implicit NULL labels.
PD3-120757801	**MPLS Packets are not Mirrored on BlackDiamond 12800 Series Switches** On BlackDiamond 12800 series switches, received MPLS packets for which an MPLS label lookup is performed are not mirrored when ingress mirroring is activated.
PD3-117148339	**Enabling or Disabling PHP on a VLAN does not Work if MPLS is Enabled** Enabling or disabling penultimate hop popping on a VLAN does not work if MPLS is enabled.
PD3-114261166	**nettx Logs When Trying to Forward 802.1Q Tagged Packets through VPLS** Port flapping, and other problems, can cause logs similar to the following when 802.1Q tagged packets are software forwarded for a VPLS service VLAN: `12/15/2006 08:11:40.67 <Erro:Kern.Error> MSM-A: nettx_vpls_transmit.(987) VPLS - problems determining .1q tag for encapsulated packet.` The logs are the result of other problems such as port flapping and will no longer appear when the other problems are corrected.
PD3-111544904	**Explicit NULL Labels are Treated as Implicit NULL Labels** When a router receives an explicit NULL label, it is incorrectly treated as an implicit NULL label, so rather than sending label 0, no label is sent.
PD3-116640291	**LDP Path Vector Limit is not Working**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
	LDP path vector loop detection may not perform as expected. For example, the LSR can advertise and propagate path vector TLVs, but will not reject FECs whose path vector value exceeds the configured path vector limit.
PD3-116409584	**LDP Path Vector Loop Detection may only Include Nexthop Path Vector LSR-ID** When enabling the LDP loop detection feature, the path vector TLVs LSR-IDs are not updated. To workaround this issue, disable and enable MPLS.
PD3-116387966	**LDP Hop Count Loop Detection may not Work Properly** LDP hop count loop detection may not work properly on transit LSRs. To workaround this issue, disable and enable MPLS.
PD3-93218551	**Packets with Router Alert Label (0x00001) are not being Forwarded** If either an egress or a transit LSP traverses the system, and an MPLS labelled packet containing a router alert label is received, that packet is not forwarded.
PD3-93069318	**VLANs Configured as Protocol "any" Should be Added to MPLS** Only VLANs configured as protocol `any` should be added to MPLS.
PD3-104731701	**ExtremeXOS does not Send back ICMP Responses for Traceroute through Non-Pipe Mode LSPs** When a traceroute is performed by setting the MPLS TTL to the IP TTL, ExtremeXOS does not correctly send back an ICMP response. The result is "*" characters in the traceroute for the routers that timed out. If a route is available, ExtremeXOS should attempt to send back an ICMP response.
PD3-93630853	**LDP Should Not Advertise Certain Label Mappings** LDP should not advertise a label mapping for a direct VLAN that does not have IP forwarding enabled.
PD3-88153931	**Pings and Traceroutes May not be Sent Using an LSP Even Though an LSP Next Hop is Available** The ExtremeXOS route table and kernel route table show that an LSP next hop for a specific route is available. However, when ping or traceroute commands are issued for a destination reached by the route, the LSP next hop may not be used.
Multicast	
PD3-184080471	**Multicast Manager Does not Update PIM after Receiving IGMPv3 Report** Multicast manager does not update an L3 VLAN with PIM enabled that is sending an IGMPv3 report.
PD3-177958011	**Switch Configured for MVR Leaks Multicast Packets to VLANs** A switch configured for MVR leaks multicast packets to VLANs that are not configured to receive multicast streams.
PD3-78144711	**"show ipstats" Command Does not Increment IGMPv3 Statistics** The `show ipstats` command does not increment IGMPv3 statistics.
PD3-79383551	**IGMPv3 Report Record Type "5" Message Does Not Work Correctly** IGMPv3 Report Record type "5" does not work as expected when sent after a type "2" or a type "4" message.
PD3-92235491	**SPT Threshold Mechanism is not Working Properly** In PIM SM, when an SPT threshold is configured as 100 Mbps, the SPT switchover may occur with 10 Mbps.
PD3-58264172	**No Entry for pimInterfaceTable When Configuring PIM**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
	When configuring PIM, there is no entry for pimInterfaceTable.
PD3-2841008	**Multicast Packets Getting Dropped when Sent at Line Rate** With PIM, when small-sized multicast streams are ingressed at line rate, there is an initial packet drop of 50% to 70%. This is seen on BlackDiamond 8810 and Summit X450 switches.
PD3-139683642, PD3-16451411	**"show pim" Command Only Counts Null-Registers** The output of the `show pim` command displays the cumulative counter for the PIM register in/out and the register-stop in/out. When the ExtremeXOS switch is a first-hop router, it sends out the real register first. After a particular mroute has been established, PIM then periodically sends the null-register. The "Register out" field does not count real registers; it only counts null-registers.
Network Login	
PD3-167032424	**Network Login Authentication Web Session Terminates after Session Refresh Times Out** A network login authentication web session terminates after a session refresh times out when moving to a nonexistent VLAN.
PD3-114466981	**Secondary RADIUS Lookup is not Used When Primary Port is Down** When the same RADIUS server is configured for both the primary and secondary RADIUS ports, using Network Login AAA authentication via the secondary RADIUS server does not work properly when the primary RADIUS port is down.
PD3-28410081	**At Line Rates, a Large Percentage of IP Multicast Packets Sent to PIM RP Will be Dropped** When sending 10,000 IP multicast packets at the line rate into DUT, only a few packets are processed and sent to the RP, causing PIM caches not to be created on the RP. If traffic is sent twice, or continuously, the PIM cache entries will be created on the RP after the initial packet los. This applies to BlackDiamond 8810 and Summit X450 switches only.
PD3-123604062	**No Response to 802.1x Request Moves Supplicant to Guest VLAN** If you configure a guest VLAN and a supplicant has 802.1x disabled and does not respond to 802.1x authentication requests from the switch, the supplicant moves to the guest VLAN of the local database.
PD3-95956875	**Network Login "move-fail-action" not Working Properly** When the move-fail-action is configured on a Network Login port as authenticate, and if a client tries to get authenticated on a tagged VLAN on the port that already exists in the same VLAN as untagged, the authentication fails because the move fails. As the move-fail-action is authenticate the client should remain authenticated in the VLAN as untagged but the client remains unauthenticated.

PD3-76900229	**Network Login Syslog Error Message**
	When Network Login is configure, the syslog should not display the following message when rebooting a Summit X450.
	`05/18/2006 15:31:10.62 <Noti:HAL.Port.Notice> aspenCardPortEnableNetlogin(1:11, 255) - Netlogin is already enabled.`
	`05/18/2006 15:31:10.62 <Noti:HAL.Port.Notice> aspenCardPortEnableNetlogin(1:10, 255) - Netlogin is already enabled.`

PD3-62154121	**Network Login Client Needs to be Reauthenticated After flush-fdb**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
	If EAPS and STP are enabled together a topology-change-notification is received by STP and can cause EAPS to flush all FDB entries on the switch. This causes Network Login clients to become unauthenticated and Web login clients, in particular, need to login again.
PD3-28603401	**Web-based Network Login Authentication through Network Login Local User Database** When web-based Network Login authenticates through the Network Login local user database, the following web Network Login features are not applied: • Default-Redirect-Page • Logout-privilege • Netlogin Session-Refresh
Network Services	
PD3-166858162	**Second Combo Port does not Come After Reboot if First combo Port is Redundant to Another Port** On a Summit X250e-24x switch, if one of the combo ports is redundant to a front panel port, after rebooting, the second combo port does not come up if the primary port for the SRP is active.
PD3-126916811, PD3-63847461	**Creating Tagged vMANs and VLANs Using the Same Ports Sends Control Packets vMAN EtherType (0x88a8)** If you create a tagged vMAN and assign two ports and then create a tagged VLAN using the same two ports, the egress port for the control packets sends the packets with vMAN EtherType (0x88a8) instead of VLAN EtherType.
PD3-100302218	**Changing Traffic Queue Mode to Bandwidth Mode Requires Two Reboots** The `unconfigure switch all` command resets the configured traffic mode. Changing the traffic mode requires another switch reboot.
PD3-104054783	**Disabling Sharing fills Console with Warning Messages** After issuing the `disable sharing` command for an LACP trunk, the following warning message fill the BlackDiamond 8800 console: `Warning: Any STP related config on the master port is lost.` `Warning: Any STP related config on the master port is lost.` `Warning: Any STP related config on the master port is lost.` `Warning: Any STP related config on the master port is lost.`
PD3-102568888, PD3-102568858	**Adding a Port to a vMAN does not Properly Enable Jumbo Frames** When a port that is disabled for a jumbo-frame is added to a vMAN using ExtremeXOS, the command line interface reports that the port was changed to being enabled for jumbo frames, but jumbo frames will not be forwarded by the switch.
PD3-93829391	**Configurations Using VR-Mgmt Interface as RADIUS Client IP Do Not Load** Configurations using a VR-Mgmt interface as a RADIUS client IP may not load at boot-up. However, using an interface in VR-Default will load correctly.
PD3-78278111	**Telnet Requests Sent from MSM-A to MSM-B Causes MSM-A to Fail** Telnet requests sent from MSM A a to MSM B causes MSM A to fail and subsequent logging through the console into MSM results in a page fault.
PD3-65041471	**Duplicate VLAN Tags will Cause Broadcast Packet to Drop** An SVLAN tag can be duplicated with other SVLAN tags as long as the ports on each SVLAN are not overlapped. The SVLAN tags cannot be the same as other regular VLAN or vMAN tags.

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
PD3-67431351	**Ingress Rate Limiting and Egress Rate Limiting are Mapping to Multiple Ports** Configuring an ingress traffic queue and an egress traffic queue association to multiple ports in sequential order generates the following error: `Egress queue already associated to this ingress queue Configuration failed on backup MSM, command execution aborted!`
PD3-67727590	**vMAN ID ACL Translations May Fail with Transmit Errors** Creating two sets of vMAN ACLs with 4000 entries each and performing a vMAN ID translation on each ACL may generate the following error: `.....03/15/2006 17:57:28.84 <Info:pm.config.openingFile> MSM-B: Loading policy RLL20k from file /config/RLL20k.pol ...03/15/2006 17:57:32.46 <Info:pm.config.loaded> MSM-B: Loaded Policy: RLL20k number of entries 4002 .....Error in alloc txmi txmi 0x9f2 txmdi 0xffffffff Error in alloc txmi txmi 0x9f4 txmdi 0xffffffff Error in alloc txmi txmi 0x1102 txmdi 0xffffffff Error in alloc txmi txmi 0x9f6 txmdi 0xffffffff Error in alloc txmi txmi 0x9f8 txmdi 0xffffffff`

PD3-67727521	**Checkpointing May Fail When Saving or Rebooting More than 4000 Traffic Queues**
	After creating 4000 traffic queues each and defining corresponding ACLs for each queue, saving and rebooting the switch may cause checkpointing to fail in the backup MSM with display the following error.
	`03/17/2006 15:07:42.64 <Info:HAL.Card.Info> MSM-A: Module in MSM-B is operational`
	`03/17/2006 15:07:45.16 <Warn:DM.Warning> MSM-A: hal: ipmlSend of DM_MSG_CHKPT_DATA failed with ipml_error -115 (errno 11)`

PD3-62778911	**Converging MVR with EAPS on a BlackDiamond 8800 Causes a Large Packet Loss** With MVR enabled on a BlackDiamond 8800, when the ingress port is on the egress-list this causes a high volume of traffic loss.
PD3-65450031	**Intra-vMAN Traffic Does not Forward on an Ingress ACL** When configuring and applying a certain ingress ACL, traffic stops forwarding to ports belonging to the same vMAN. Removing the ingress ACL restores traffic.
PD3-64743301	**Configuring a Meter Value not Working Properly on a BlackDiamond 12804** When configuring a meter value using a large number, for example, 10,000 Gbps, on a BlackDiamond 12804 switch the CLI accepts the command. However, when you run the `show meter` command, an incorrect value is displayed.
PD3-58240961	**Extreme Networks Uses the Value 0x88B6 for the Ethernet Type for CFM** Extreme Networks is currently using the value 0x88B6 for the Ethernet type for CFM as the IEEE 802.1ag.
PD3-52741643	**Disabling Load Sharing May Cause Temporary State Change** Enabling/disabling load sharing on ports while ESRP is running may cause temporary state changes.
PD3-46782671	**Configuring an SSL Certificate Automatically Enables HTTPS** When an SSL certificate is configured, it automatically enables HTTPS. However, the show ssl command can show HTTPS as disabled.
PD3-56415901, PD3-42385251	**Switch May Stop Responding When Traffic Hits a Large ACL Policy**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
	When creating a large policy file on a BlackDiamond 10808 switch and applying the policy to a VLAN on egress, if traffic is sent that attempts to hit the ACL rules, and the next hop ARP entry is not yet learned, the MSMs may stop responding.
PD2-205017587, PD2- 197340001	**VLAN Statistic for rtif Interface is not Displayed** The VLAN statistic for the rtif interface is not displayed in ifTable/ifXTable.
PD3-46069035, PD3-35996092	**Disabling Smart Redundancy** After disabling smart redundancy on a port and then configuring the port and creating a VLAN, when you issue the `show vlan` command, the output displays *p1, *p2b. However, after you save the configuration and reboot the switch, the DUT may display `*p1b, *p2`.
PD2-223515075	**VLAN Mirroring Not Functioning Properly** VLAN mirroring does not work once you change the VLAN tag.
PD3-29034388	**Clearing Neighbor Cache Can Cause Packet Drops** Clearing a neighbor cache with line rate traffic may cause delays in re-establishing the neighbor cache, which can result in packet drops. The delay can be avoided by temporarily pausing the line rate traffic, thereby allowing the neighbor cache to be re-established.
OSPF	
PD3-133427241	**OSPF Filter not Filtering all Routes** When an OSPF external filter is configured to deny routes, not all routes are being filtered.
PD3-42948087	**Changing Time While OSPFv3 is Learning Can Cause LSA to not Generate** If the system time is changed while OSPFv3 is running, LSAs may not generate and the routes may not be learned. To avoid this, run the `disable ospfv3` command followed by the `enable ospfv3` command to start OSPFv3 functioning properly.
Policy Manager	
PD3-29818741	**ETHER-P-8021Q is Not a Valid Match Criteria** ETHER-P-8021Q is not a valid ethernet-type match criteria and generates a syntax error. You can use 0x8100.

PD3-47374991	**Incorrect Error Message When an Incorrect Policy is Configured Using BGP**
	The following incorrect error message is displayed when configuring a route policy using BGP:
	`* BD-10808.7 # config bgp neighbor 55.15.15.100 route-policy out nosales`
	`BGP: Bind policy "nosales" failed!`
	`No Error <<<<<<`
	`Configuration failed on backup MSM, command execution aborted!`
	`* BD-10808.8 #`

QoS	
PD3-129177287	**If IRL-ERL Traffic Queue Mapping Extends to all Ports, Port Selection is Void** Create an ingress traffic-queue with allow egress shaping and create an egress traffic-queue. Map the IRL to ERL on all ports. Send unidirectional traffic, which should hit the IRL rule at ingress. The same traffic is visible to the ERL at the egress port without selecting the designated port of VLAN/vMAN.

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
PD3-35119459, PD3-22513166	**Changing the Default Queue Profiles** The default queue profiles mapping remain intact even after deleting and adding the QoS profile on a Summit X450 or BlackDiamond 8800 switch.
PD3-16578296	**Disabling Load Sharing or Deleting Member Ports from a Trunk** The member ports of a trunk will retain the QoS profile configuration of the trunk (based on the master port) after load sharing is disabled, or if a port is removed from the trunk.
RIPng	
PD3-54863764, PD3-41040185	**No Warning Message When Configuring More than 512 RIPng Interfaces** Configuring more than 512 RIPng interfaces on a BlackDiamond 10808 generates the following error message: `Configuration failed on backup MSM, command execution aborted!` On a BlackDiamond 8806 or Summit X450 switch, although only 512 RIPng interfaces are configured, there is no warning message that the command failed.
RMON	
PD3-17622009, PD3-20727420	**Trap Community String Octet Limits for Agent is Not Correct** trapDestCommunity allows octet string (0..127) but agent only support 32 characters strings.
PD3-12950492	**"clear counter" Command Not Supported** Issuing the `clear counter` command might cause a high number to be displayed in variables such as etherHistoryOctets, etherHistoryPkts, and etherHistoryTable.
PD3-17091355	**Alarm Entries Not Being Generated Correctly** Creating an alarm entry with an initial value of 0 for the alarm generates a falling alarm.

PD3-63584999	**Policies Configured on MVR Cannot be Refreshed**
	Do not refresh a policy configured on MVR. The workaround is to unconfigure and reconfigure the policy. For example:
	`configure mvr vlan v1 static group none`
	`configure mvr vlan v1 static group <policy-name>`

ScreenPlay	
PD3-182346729	**WebUI/Screenplay displays Telnet Access Based on SSH Configuration.** WebUI/Screenplay displays telnet access as enabled or disabled based on the SSH configuration instead of the CLI telnet configuration.
PD3-135174293	**VR should be Read-Only** VR should be a read-only attribute when editing a VLAN in edit mode.
PD3-111344472	**Cannot Enable DHCP using WebUI** ScreenPlay allows you to configure DHCP but you cannot enable DHCP.
Security	
PD3-185470912	**Users cannot Receive IP Address from DHCP Server** Users are unable to receive IP addresses from an ExtremeXOS DHCP server over load sharing port.
PD3-102617597	**Cannot Use Special Characters when Defining RADIUS Shared-Secret Key**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
	Special characters such as <, >, &, ?, and / cannot be used when defining a RADIUS shared-secret key.
PD3-133763260	**New Backup MSM Reboots Twice after Failover** A new backup MSM reboots twice after failover (`run MSM-failover`). The backup MSM initially comes up correctly but is not in the "In SYNC" state. The MSM then reboots without a core and comes up "In Sync" on a BlackDiamond 8800. This problem does not occur consistently and should not affect data transmission. It is recommended that you disable the notify function in the `disable ip-security anomaly-protection notify <log | cache | snmp>` command to avoid potential problems.
PD3-128752502	**Anomaly Counters Stop Counting** After issuing the `enable ip-security anomaly notify <log | cache | snmp>` command, the anomaly counters `show port <port-list> anomaly` stop counting. The anomaly violation counters in the `show port <port-list> anomaly` command will stop counting after the `notify` function is enabled (`enable ip-security anomaly-protection notify <log | cache | snmp>`). Disabling the `notify` function restores counting.
PD3-118747911	**Portions of the IP Security Feature set are not Supported with Static IP Addresses** The DHCP snooping, source IP lockdown, and DHCP secured ARP portions of the IP security feature set depend on DHCP assigned IP addresses and are therefore not supported with clients having static IP addresses.
PD3-124968250	**Load Script Defaults TACACS Configuration to VR-Mgmt** Load script defaults the TACACS configuration to VR-Mgmt even when VR-Default is specified.
PD3-110736351	**RSA Key not Supported** When configuring SSH, use only the DSA public key. The RSA key is not supported in ExtremeXOS 12.0.
PD3-109022651	**Enabling IP Security on Link Aggregation Ports is not Supported** Enabling IP security features on link aggregation ports is not supported In ExtremeXOS 12.0. However, the CLI still allows configuring these features on link aggregation ports.
PD3-102073084	**Authentication Using Dummy Primary and Secondary Servers Fails** Configure a dummy primary server and issue the show session and show radius commands. This should take approximately 14 seconds to execute. Running the same commands with a dummy secondary server takes approximately 15 seconds to execute. If you log out and log back into the switch it will take 15 seconds. During this time, multiple counters are incrementing in the show radius command output.
PD3-96212671	**DHCP Packets are not Relayed if dhcp-snooping violation-action is Set to None** When DHCP snooping is enabled on a port in a VLAN in monitoring only mode (that is, with the violation-action option set to none) and the switch is acting as a BOOTP relay, DHCP packets are not relayed from the DHCP server on that port. As a workaround, the port can be configured as a trusted-port (trusted for DHCP server packets) with DHCP snooping enabled with a violation-action of drop-packet instead of none. This works the same as setting the violation-action to none viz. The DHCP bindings database is built up by monitoring DHCP traffic but no rogue DHCP server traffic on that port is dropped.
PD3-77320136	**RADIUS NAS-Port Attribute Should Display Without Slot Information** The RADIUS NAS-port attribute displays the port as 1024, instead of port 24.

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
Security	
PD3-77320118	**RADIUS NAS-Port Attribute is Missing for Network Login RADIUS Access Request Packets** The RADIUS NAS-port attribute is missing for Network Login RADIUS access request packets, but is included in the accounting packets.
PD3-75465301	**"unconfigure radius" Command is not Clearing RADIUS Authentication and Accounting Counters** The `unconfigure radius` command does not clear the RADIUS authentication and accounting counters.
PD3-75120608	**Unconfigure RADIUS and TACACS Does not Reset Timeout Value to System Default** The `unconfigure radius` and `unconfigure tacacs` commands do not reset the timeout value to the system default of 3 seconds.
PD3-74708933	**RADIUS Authentication do not Work Correctly if Console Accesses the Backup MSM** If you are configuring a BlackDiamond 10808 or BlackDiamond 8810 with RADIUS authentication, when telnet or console access is through the master MSM, RADIUS authentication works correctly. However, if console access is through the backup MSM, RADIUS authentication does not work correctly and generates the following error message: `<Erro:AAA.RADIUS.serverNotInit> MSM-B: Authentication server for Switch Management is not initialized`
PD3-29911678, PD3-29948301	**Changing a Password after Password Expiration Terminates SSH Session** When a local user password expires, logging into the switch using SSH will prompt you to change your password. After changing the password, the current SSH session will be terminated and you will need to login to the switch using the new password.
PD3-40462478, PD3-27536575	**sFlow Will Accept Invalid IP Addresses for Collector Address** sFlow allows you to configure invalid IP addresses as sFlow collectors. Only valid unicast IP addresses should be used to configure the sFlow collector.
PD3-19287440	**sFlow May Not Sample Correctly with Heavy Traffic** sFlow will under sample packets on BlackDiamond 8800 original series I/O modules and Summit X450 switches except during periods of very light ingress traffic on the specified port. This problem does not apply to BlackDiamond 8800 a-series and e-series modules or Summit X450a and X450e series switches.
SNMP	
PD3-181304741	**entPhysicalDescr MIB for XENPAK Modules Always Shown as XGM-** After inserting a XENPAK in a stack (XGM2-2xn, XGM-2xn) and performing an snmpwalk on the entityMib entPhysicalDescr variable, XGM- is always shown, not the complete module description.
PD3-176649686	**Switch Becomes an L3 Device if IP Forwarding is Enabled on Any VLAN** The MIB object ID 1.3.6.1.2.1.4.1.0 returns a switch as an L3 device if IP forwarding is enabled on any one VLAN.
PD2-204685753, PD2-196089286	**extremePortLoadshare MIB Table Empty When Load Sharing is Enabled** Enable load sharing on a port and run the `show ports configuration` command. Even though the command output shows that load sharing is enabled on the port, the extremePortLoadshare table is empty.

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
PD3-39411271	**icmpInMsgs Counter Displays only Incoming ICMP Packets** icmpInMsgs counter will display the incoming ICMP packets for VR-Default only.
PD3-118437141	**MIB extremeVlanIfStatus Shows VLAN Always Active even when VLAN is Disabled** Polling the extremeVlanIfStatus (object OID .1.3.6.1.4.1.1916.1.2.1.2.1.6) always returns a result of active for a VLAN interface. Even when the VLAN is disabled, or does not have an active port, the switch returns "active." The result should be "not ready" or "not in service."
PD3-47804527	**Smart Traps not Generated while Adding a Trap Rule IP Address** Smart traps are not generated if the smart trap rule ipAddrTable is configured.
PD3-42395376	**Some Objects in icmpGroup May Return Incorrect Values** When initiating an outgoing ping from the switch, the following counters do not increment: • icmpOutMsgs • icmpOutEchoReps
Spanning Tree Protocol	

PD3-183228011	**MSTP Configuration Example Correction**
	The configuration example shown on page 735 of the *ExtremeXOS 12.0 Concepts Guide* should read:
	In the following example, the commands configure Switch E in Region 2 for MSTP. Use the same commands to configure each switch in Region 2:
	`create vlan finance`
	`configure vlan finance tag 2`
	`configure vlan finance add port 2-3 tagged`
	`configure mstp region region2`
	`create stpd s0 (Default)`
	`configure stpd s0 mode mstp cist`
	`configure stpd s0 priority 32768 (Default)`
	`enable stpd s0`
	`create stpd s1`
	`configure stpd s1 mode mstp msti 1`
	`configure stpd s1 priority 32768 (Default)`
	`enable stpd s1 auto-bind vlan finance`
	`configure stpd s1 ports link-type point-to-point 2-3`
	`enable stpd s1`
	In the following example, the commands configure switch D, the external switch. Switch D becomes the
	`CIST root bridge:`
	`create stpd s0 (Default)`
	`configure stpd s0 mode dot1w`
	`configure stpd s0 priority 28672`
	`enable stpd s0 auto-bind vlan Default`
	`configure stpd s0 ports link-type point-to-point 4-5`
	`enable stpd s0`
	This correction will be made in the *ExtremeXOS 12.1 Concepts Guide.*

PD3-177657971	**MSTP BPDU Does not Contain MSTI Messages, Causing Port Status to be Boundary Instead of Internal**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
	When configuring MSTP on different ports in the same CIST and MSTI region, the port status changes to Boundary and generates the following log message in the STP logs: `09/18/2007 09:52:58.03 <Verb:STP.State.Handshake> MSM-A: [s1:3:3] RSTP BPDU: No MSTI instance found to piggiback M-Record` The port status must be Internal.
PD3-157231492, PD3-156787152	**Edge Safeguard does not Block a Port** Even when edge safeguard is enabled on an edge port and a loop is detected, edge safeguard does not block the port.
PD3-123227322	**CLI Does not Show a Clear Error Message when Configuring STP** When the same port is added in dot1d mode to two different STP domains, ExtremeXOS switches are not providing a clear error message.
SSH and SSH2	
PD3-29939091	**ssh.xmod Must be Installed to Configure SSL Certificates** ssh.xmod must be installed to configure SSL certificates. If ssh.xmod is not installed on the switch, configured SSL certificates are not loaded into the switch and no error is returned.
PD3-20944751, PD3-14620801	**Regenerating an SSH Key** After regenerating the SSH key you must save the configuration and then terminate SSH. Terminate the SSH process using the `terminate process exsshd graceful` command and then restart the process using the `start process exsshd` command.

PD3-60673957, PD3-39739546, PD3-26746401	**DES Cipher Fails Authentication**
	Attempting to login to the switch with a "des" cipher fails authentication and generates the following message:
	`warning: Authentication failed.`
	`Disconnected; key exchange or algorithm negotiation failed.`

Stacking	
PD3-126815409	**"configure sys-recovery-level slot" Option Does Not Work** The `configure sys-recovery-level slot` command does not currently work on stack slots.
PD3-138014104	**Stack Reboot is Possible During an Image Upgrade or Configuration Save Is In Progress** You can run the `reboot stack-topology` command on any stacking switch while the master switch is downloading or installing an image, or saving a configuration file. This results in incomplete file operations before the reboot takes place, which may render the image or configuration unusable. Be sure that neither operation is in progress when rebooting the stack.
PD3-136493921	**AAA Services Do not Become Available on Stacking Switch that has a Mismatched License**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description
	If a switch is added to a stack whose master switch has a license level that is greater than the level of the switch, the switch will fail. The complete condition can be seen using the `show slot detail` command. In this state, the switch does not have AAA services available. You will only be able to log into the switch using the failsafe account that was last assigned to it. You must log into the switch to upgrade the license. If the switch is not using the failsafe account configured on the stack, you can use the `synchronize stacking {node-address <node-address> | slot <slot-number>}` command to copy the failsafe account information from the master switch to the failed switch NVRAM. You can also use the `configure stacking license-level` command to configure a license level restriction on the entire stack and then reboot the stack. Once the stack is restarted, there is no longer a license mismatch, enabling you to log into the switch and upgrade the license. From the master switch, run the `unconfigure stacking license-level` command to get the stack to operate at the desired license and then reboot the stack.
PD3-133978700, PD3-138140417, PD3-137976136	**Quick Stacking Cable Removal and Insertion Problem** If you remove and quickly replace the stacking cable causing a separation of one or more switches from the stack, the stack master may not consistently detect the missing slots. The system may try to reinitialize the slots without first performing the necessary reboot. Extreme Networks recommends that you wait at least five seconds between removing the cable and replacing it again.
PD3-126650411	**Stackable Systems with Two or More Nodes may Experience Random VRRP Master/Backup Flapping** A stackable system with two or more nodes may experience random VRRP master/backup flapping issues after an MSM failover when configured with the maximum 128 VRRP instances using the minimum advertisement interval of 100ms and maximum tracking entries.
PD3-119233421	**Ports are not Added when Creating VLANs in a Stack** VLANs can only be created if there is at least 20MB of main memory available. A port can only be added to a VLAN if there is at least 30MB of memory available. Currently, one of these limits will be encountered if approximately 2,500 VLANs with eight ports each are configured evenly. Changing the order in which VLANs are created and ports are added may result in different configurations at the time a limit is encountered. Also, since memory is shared with other features, for example, route tables, the number of VLANs and ports that can be created may be considerably lower.
System Related	
PD2-241021669, PD2-222627405, PD2-210437928	**Static Route Forwarding Does Not Forward to a Second Link** In a multiple switch configuration, if two switches have two links and share static route forwarding, if the first link forwarding traffic has ipforwarding disabled, the traffic does not resume with the second link that still has ipforwarding enabled.
PD3-28577971	**show log Error Messages**

Table 33: Feature-Specific PDs (Continued)

PD Number	Description

	Messages stored in NVRAM are in encoded format. To restore the ASCII text of a message, the version of ExtremeXOS loaded must be able to interpret the data written prior to reboot. When the encoded format for a particular message cannot be interpreted by the version of ExtremeXOS currently loaded, the messages are displayed in the following format.
	`03/21/2005 17:15:37.36 <UNKNW:epm.28>: NO MESSAGE DECODE; Missing component "epm" v24.2`
	`DUMP-00: 00 2C 00 01 FF FF FF FF 00 00 00 95 42 3F 71 B9`
	`'.,..........B?q.'`
	`DUMP-10: 00 14 C3 C1 00 11 00 1C 01 FF 00 08 65 70 6D 00`
	`'............epm.'`
	`DUMP-20: 08 FF 00 0C 00 18 00 02 65 70 6D 00`
	`'........epm.'`

PD3-28631368	**Unknown Card Type Error Message** The following message is displayed on the console when a module is present that the current image does not support: `Error: Unknown card type in slot X, please remove!` ExtremeXOS will not check-point sync the switch until the incorrect module is removed.
UPM	
PD3-177997561	**Cannot Enable/Disable PoE in Non-Persistent Mode for UPM** Enabling and disabling PoE does not work in non-persistent mode for UPM.
PD3-124182761	**LLDP is Showing Power in Tenths of a Watt** The variable EVENT.DEVICE_POWER now displays power in milliwatts when an LLDP device is detected. For example, 5.7 watts is now shown as 5700.
VRRP	
PD3-95689131	**VRRP is not supported on User-Created VRs** VRRP is not supported on user-created VRs in ExtremeXOS 12.0.2.
PD3-54695903	**MSM Failover on VRRP Backup Node Causes VRRP State Change** An MSM failover causes a VRRP state change when running 128 virtual routers in the backup state on a BlackDiamond 8800 and a BlackDiamond 12804.
PD3-54852211, PD3-41952782	**Data Packets will not be Forwarded When Configuring VRRP with vrid >=7** On a BlackDiamond 10808, if you configure VRRP with seven unique VRIDs, and configure one or more ESRP domains, data packets will not be forwarded on one of the eight virtual MACs. Therefore, when the last domain is enabled, it will not be allocated a virtual MAC and will not forward traffic. The domain that will not forward traffic will be the last domain that is enabled, which can vary. To avoid this situation, do not configure ESRP and VRRP at the same time.
WAN PHY	
PD3-101226461	**WAN PHY "show" Commands Should not be Applied to non WAN PHY Ports** When `show wan-phy` commands are issued on non WAN PHY ports, the ports display the headers. It should only display the error `wan command is not supported on non-wanphy port 25`.

Issues Resolved in ExtremeXOS 12.0.2.25

The following issues were resolved in ExtremeXOS 12.0.2.25. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.0 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, and ExtremeXOS 11.6.3.5. For information on those fixes, see the release notes for the specific release.

PD Number	Description
Summit Family of Switches	
PD3-178103151, PD3-126844141	Combo ports only allow the supported 1 gigabyte configurations on LX100 mini GBIC modules. An error is logged for invalid speeds.
Security	
PD3-118069689	The `show ports anomaly` command output is now correct for ingress traffic.

Issues Resolved in ExtremeXOS 12.0.2.18

The following issues were resolved in ExtremeXOS 12.0.2.18. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.0 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, and ExtremeXOS 11.6.3.5. For information on those fixes, see the release notes for the specific release.

Table 34: Platform-Specific and Feature PDs

PD Number	Description
General	
PD3-179244891	The `debug hal show platform platformInfo` command no longer displays garbled and truncated output.
PD3-141735501, PD3-140703992, PD3-153125358	Consecutively uploading an image to a switch using SFTP followed by entering the install image command, without terminating the original SSH session, no longer causes the switch to reboot during the installation

PD3-176609012	Summit X450a and X450e series, and BlackDiamond a-series and e-series switches no longer erroneously display table add failures and log messages such as:
	`Slot-8: unit 0: Internal error: could not add L3 table entry 0x9DCCE16A`
	`Slot-1: Unable to Del IPmc sender entry s,G,v=c0a896d4,ef53646d,1 IPMC 9 unit 1, Internal error.`

PD3-176453632	Disabling an I/O port on an MSM G8X module now takes the link down at the remote end.
PD3-177856491	The hardware setting for learning on Summit X450a and X450e series switches and BlackDiamond 8800 a-series and e-series modules no longer affects MAC addresses from being properly learned and displayed in the `show fdb` command output.
PD3-174974331	ExtremeXOS 12.0 now supports installing (*,G,V) entries in hardware in order to save IP multicast forwarding database space.
PD3-168827110, PD3-149672166	In an L3 routing enabled configuration, a topology change for multicast traffic flow no longer causes the corruption of the port list maintained in hardware for flooding broadcast/unknown destination MAC traffic on BlackDiamond 10808 and BlackDiamond 12800 switches.

Table 34: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-118365873	An image installation failure no longer occurs when trying to upgrade from images later than ExtremeXOS 11.2 to ExtremeXOS 11.4.3, or later, without first upgrading to ExtremeXOS 11.2.1.
BlackDiamond 8800 Series of Switches	
PD3-155071953	Ping no longer fails after an MSM failover if the ports in the load-sharing group are on MSM-A and MSM-B.
BlackDiamond 10808 Switch	
PD3-177356531	An MSM failover caused by a deadlock in the CPU packet driver is no longer seen
PD3-168765821	Continuously sending IGMP join/leave requests to multiple groups no longer depletes the memory consumed by PIM and MSDP processes
Summit Family of Switches	
PD3-159765751	Running diagnostics on a Summit X250e-24x switch with an active port no longer generates a diagnostics failure error.
PD3-172062316	It no longer takes five to six seconds to perform an MSTP convergence on two regions
PD3-131382916	Disabling autopolarity still no longer allows a link to come up between two switches when you are using a straight-through cable.
PD3-127957781	A Summit X450 series switch no longer logs a link down event showing Local fault as the reason for the event. The link down event applies to each 10G XENPAK port present on reboot when the cable is connected to both the local (near-end) and remote (far-end) ports.
ACL	
PD3-173103143	An ACL crash no longer occurs during a policy refresh if the ACL counter name is 32 characters.
BGP	
PD3-138248301	Blackhole routes are no longer removed whenever an aggregate statement from a BGP neighbor is added or removed
PD3-168814611, PD3-120895991	A BGP neighbor IP address check is no longer performed per classful network.
PD3-138333691	Running the `configure bgp add aggregate-address summary-only` command no longer results in component routes being sent.
PD3-138248301	Blackhole routes are no longer removed whenever an aggregate statement from a BGP neighbor is added or removed.
Device Management	
PD3-120925819	Running the `configure protocol any (llc, etype, snap)` command no longer causes the switch to crash.
IGMP	
PD3-172905626, PD3-169760051	Sending an IGMP report for a port that is otherwise reserved for multicast DNS, no longer causes the port to become a router port, which was resulting in all multicast traffic being forwarded on that port in a VLAN.
IP Routing Protocols	
PD3-149955482, PD3-160238953	BGP nexthop resolution no longer fails when a direct route with a length of 25 for nexthops is resolved
PD3-155226621	A new CLI command, `enable/disable igmp proxy-query vlan <vlanname>`, has been introduced to enable and disable sending IGMP proxy queries with an L2 VLAN.
IP Unicast	

Table 34: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-166964541	ECMP routes now only consume L3 hash table entries on original Summit X450 switches with the Summit XGM-2xn option card, or on 10G4X modules in a BlackDiamond 8800 series of switches.
PD3-166964776	A new value of max-gateways 2 has been added to the `configure iproute sharing max-gateways` command that will allow 1,024 ECMP route sets in hardware with up to two gateways each. This is in addition to the existing choices of 4 and 8, and applies to the BlackDiamond 8800 series of switches, Summit family of switches, and SummitStack only.
IPv4 Multicast	
PD3-168847771, PD3-156370064	Multicast cache entries are now updated in hardware after an MSM failover.
PD3-168826871, PD3-125375605	Egress port information in the hardware IPv4 multicast cache entry is no longer out of sync with the software IPv4 multicast cache entry on the BlackDiamond 10808 switch and the BlackDiamond 12800 series switches.
PD3-160528665	In a triangle topology, multicast packets are no longer forwarded out of STP blocked ports until the IGMP snooping cache entries age out.
MPLS	
PD3-130584481	Running LDP and 3,000 labels no longer generates an error message.
PD3-76640281	Sending a 100 Mbps data stream with a destination address of broadcast on a Virtual Private LAN Service (VPLS), no longer causes the Label Distribution Protocol (LDP) to flap.
PD3-97185211	Classifying MPLS packets based on EXP field examination and EXP field replacement are now supported.
PD3-121740899	A VPLS session no longer goes down and fails to come back up if an IP MTU is changed while a VPLS session is operationally up.
PD3-123285381	An SNMP trap is now generated for each blackholed FDB entry after reaching the MAC learning limit for a VPLS peer.
PD3-128400391, PD3-137613771	Continuously disabling and enabling MPLS using the `disable mpls` and `enable mpls` commands no longer leads to a memory resource shortage.
Multicast	
PD3-168766009	PIM now populates the MSDP local cache when PIM has (S,G) cache entries.
PD3-168765953	The `clear pim cache` command no longer causes a PIM process crash when multicast traffic is being sent and join/leave messages are being received.
PD3-168765907	A PIM assert no longer occurs every 60 seconds when a non-designated router becomes the designated router and then reverts back to the non-designated router, which was causing an assert loser situation.
PD3-168847506, PD3-160496014	When a multicast stream source MAC IP address ages out in an FDB (30 seconds), if the same multicast stream starts again, the packets are no longer dual forwarded by fast path and slow path.
Network Login	
PD3-142971731	When a web-based Network Login user logs out, the switch retains the existing IP address. However, the IP address must be released so that the switch can provision a temporary IP address of its own for correct Network Login functionality while the user is in the unauthenticated state. Since the switch does not automatically trigger an IP release and renew, the user must manually perform the release and renew. This does not affect switch performance.
Network Services	
PD3-135376601	The loopback port LED now lights on the BlackDiamond 12800 series switches after enabling mirroring.
PD3-131127794	All external cables connected to a configured loopback port no longer need to be disconnected before you start mirroring.

Table 34: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-158749466	Configuring a password with eight characters no longer displays an error message when enabling VRRP.
Network Tools	
PD3-152513845, PD3-152169000	ExtremeXOS shell process (exsh) invoked by the telnet session is now terminated after the session is closed.
Security	
PD3-135530701, PD3-135845805	On certain platforms and modules, when IP security features are enabled in a BOOTP Relay setup, DHCP snooping and associated entries are now removed by a DHCP release.
Spanning Tree Protocol	
PD3-135431781	RSTP with pvst+ port mode is now also supported on third party switches.
PD3-154757941	The RSTP edge safeguard feature can now be used to protect untagged edge ports.
SSH	
PD3-174930634	The SSH process exsshd no longer consumes too much CPU usage after a system reboot.
Stacking	
PD3-120499891	Enabling and disabling network login on a port list no longer generates error messages in the log.
PD3-137283332	The `reboot slot` and `run failover` commands take about three seconds to complete. That is at the edge of the default master-down time of 3 * 1 second advertisement, or three seconds. As such, the commands no longer cause a VRRP mastership change when the default of one second advertisement is used because the timer may expire.
PD3-126548889	The command output for the `show ports stack-ports` command no longer incorrectly shows down ports as Active (A). The ports are now shown as Ready "R."

Issues Resolved in ExtremeXOS 12.0.1.11

The following issues were resolved in ExtremeXOS 12.0.1.11. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.0 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, and ExtremeXOS 11.6.2.9. For information on those fixes, see the release notes for the specific release.

Table 35: General and Platform-Specific Resolved Issues

PD Number	Description
General	
PD3-128551591	While upgrading to ExtremeXOS 12.0 from an earlier release of ExtremeXOS software, the `show version` command now shows the correct version.
PD3-133203289	ExtremeXOS suppresses log messages for spurious AC PSU input voltage readings. A single spurious value reported by an AC PSU is ignored by ExtremeXOS rather than logged as an increase in voltage, immediately followed by a decrease in voltage. This occurs on BlackDiamond 8800, BlackDiamond 10808, and BlackDiamond 12804 switches.
BlackDiamond 8800 Series Switches	
PD3-125375611	The `configure vlan protocol ipv6` command displays in the `show configuration` command output.
PD3-94962493	A conduit receive error no longer occurs on MSM slots when performing an MSM failover.

Table 35: General and Platform-Specific Resolved Issues (Continued)

PD Number	Description
PD3-86869211	For ports on Summit X450 switches and BlackDiamond 8800 MSM-G8X, G48T, G48P and G24X modules, the RX Over counter is now incremented when ports are connected at 100 Mbps.
PD3-78998371	IPv6 traffic is no longer slowpath forwarded while ingressing on the BlackDiamond 8800 original series modules, which was causing the CPU to be unable to keep up with both the IPv6 traffic and the OSPFv3 handshaking, causing adjacencies to be lost.
PD3-60122761	Hot swapping a 10G4X or G24X I/O module in a BlackDiamond 8810 no longer allows the link peer to prematurely get an active link state. If this port is configured as an EAPS shared port, a temporary loop was seen in the network. This problem has been corrected on G48Xa and 10G4Xa modules only.
PD3-45929245	When routing between VLANs on a BlackDiamond 8800 original series or Summit X450 series switch, ingress mirrored traffic is no longer presented to the monitor port as having been modified for routing.
PD3-128654641	The `disable rip` command no longer causes the CLI to hang on a BlackDiamond 8800 series switch with a G48T module.
BlackDiamond 10808 Switch	
PD3-93088150	A BlackDiamond 10808 using 64 ESRP domains and 512 VLANs, no longer generates a HAL core during the save and reboot commands.
BlackDiamond 12800 Series Switches	
PD3-126533672	After rebooting a BlackDiamond 12804 with continuos traffic flowing, MSM B no longer takes too much time to come up.
PD3-67969258, PD3-61635051	Running the `clear slot` command on a system with large configurations no longer takes a long time to process.
PD3-63913145	Downloading a new image on a BlackDiamond 12804 no longer generates a log message.
PD3-63887081	At initial bootup, the BlackDiamond 12804R no longer prompts a user as to whether or not to disable all ports on the switch. All ports are disabled after initial bootup until the user responds to enable all ports.
PD3-121372064	When you configure three different services and send traffic with a peak rate for all services, 200M of traffic is no longer sent out on an egress port instead of the expected 100M.
Summit Family of Switches	
PD3-92509429	A Summit X450 series switch no longer displays an insufficient power message when performing a cold boot.
PD3-89711032	When rebooting a Summit X450-24x, neighboring switches connected to the fiber port no longer experience a link flap before the switch is in the operational state.
PD3-129614671	A `No TX match` error is no longer occasionally seen when running diagnostics on a Summit X450a-24x or X450e-24p switch.
PD3-78030636	If you use the `clear sys-recovery-level` command on the Summit X450a and X450e series switches, a warning message is no longer displayed.
PD3-98415064	It is no longer necessary to save your configuration after configuring sys-health-recovery level to shutdown to ensure proper operation of the feature.
PD3-103618060	On a Summit X450 switch, when autonegotiation is On, disabling and enabling a port on a 100FX module no longer displays the wrong speed.
PD3-87341149, PD3-77237152	The management port is no longer reported as down when it is in the shutdown state but is actually working correctly. When a Summit X450 switch is in shutdown state, all ports must be down with the exception of the management port.
ACL	
PD3-79357521	Adding a large number of dynamic ACLs as "priority first" no longer fails.
PD3-104389194	IP security ACLs are now shown in the `show access-list vlan` command output.

Table 35: General and Platform-Specific Resolved Issues (Continued)

PD Number	Description
PD3-58209747	The ACL action replace-dscp is now taking effect when traffic egresses on a second switch.
PD3-58149031	Configuring dynamic ACL Ethernet Subnetwork Access Protocol (SNAP) packets no longer causes the wrong dynamic ACL counters to increment.
CLI	
PD3-67968832	The `show odometers` command now displays PSUCTRL service days.
PD3-61996631	The CLI command `enable ipforwarding fast-direct-broadcast | ignore-broadcast` is now supported on a BlackDiamond 10808 switch.
Control Protocols	
PD3-129126971	The aggregated port cost of a Summit X250e peer is no longer changed by disabling one aggregated link.
Device Management	
PD3-77979260, PD3-77847804	The `configure-sys-recovery level slot shutdown` command can now be used on an MSM slot.
PD2-204940185	Logging into the backup MSM-console no longer fails to local authentication when using RADIUS/TACACS authentication.
PD3-95714861	The switch no longer displays extraneous errors when loading non-existent variables.
PD3-95643404	When installing a ZX mini-GBIC into a mini-GBIC port on the Summit X450e-48p switch, the switch no longer displays it as an LX mini-GBIC.
EAPS	
PD3-20733191	If a BlackDiamond 8810 system is running heavy unicast or multicast traffic, or has a large amount of FDB or IPMC cache entries, bringing the EAPS ring port down and up frequently may cause both the EAPS primary and secondary ports to be blocked for several seconds only.
PD3-95187020, PD3-72086161	EAPS warning messages are no longer displayed from the VLAN manager after running the configure eaps config-warnings off command.
ESRP	
PD3-35920481	Summit X450 now shows ESRP-aware information in the summary display.
PD3-103123831	An MSM failover from an ESRP master no longer causes an FDB flush on the new master during the pre-master to master transition.
PD3-83773893	An MSM failover on a BlackDiamond 10808 that is operating as an ESRP master no longer triggers an ESRP mastership change, causing the switch to become an ESRP slave.
IP Routing Protocols	
PD3-128929252	Disabling IP route sharing no longer causes incorrect behavior in route compression.
PD3-90712545	MVR now sends periodic IGMP reports if the MVR VLAN is an L2 VLAN and configured static router.
IPv6 Unicast	
PD3-78254454	IPv6 FIB and adjacency entries are no longer cleared when a duplicate IPv6 address is detected (DAD).
PD3-126009211, PD3-78254331	Adding Neighbor Discovery Cache entries matching an existing VLAN IPv6 address in the switch is not allowed. Static neighbor discovery entries can be created for the IPv6 addresses of neighboring switches for any of the VLANs.
PD3-79041026	On the BlackDiamond 10808, BlackDiamond 12804, BlackDiamond 12802, Summit X450a, Summit X450e, and Summit X250e switches, and in the BlackDiamond 8800 a- and e- series modules, IPv6 packets for IPv6-in-IPv4 and 6-to-4 tunnels are no longer forwarded in software. The packets are now correctly forwarded at line rate.
MPLS	

Table 35: General and Platform-Specific Resolved Issues (Continued)

PD Number	Description
PD3-125916164	LDP sessions no longer flap between operational and non-existent because of missing hello packets after an MSM failover.
PD3-125916129	The switch no longer experiences high packet loss when issuing the `run msm-failover` command numerous times on the ingress/egress switch.
PD3-125508231	MPLS now sends data to OSPF after OSPF restarts.
PD3-121098111	Link flapping and other similar issues no longer cause an LSP ping to generate an error log message.
PD3-118425312	After running the `run msm-failover` command, traffic completely recovers in both directions.
PD3-117124291	The `show mpls ldp peer <lsr-id>` command now shows a peer if the peer is using an interface label space.
PD3-114996515	Changing a VLAN from tagged to untagged may result in LDP not advertising a label for that VLAN.
PD3-111544750	On a BlackDiamond 10808, the counters from ports mapped to the backup MSM are now included in the VPLS and LSP output for received bytes and packets shown in the command output for the `show mpls ldp lsp detail`, `show mpls rsvp-te lsp`, and `show vpls detail` commands.
PD3-110196861	The `clear counters` command, or variations of the command, no longer result in MPLS HAL log messages.
PD3-104046299	When an OSPF database exchange occurs, if the LSID for the OSPF router address has changed and the neighbor's version must be flushed, for example, after a reboot, the router address is no longer purged from the CSPF database.
PD3-100051127, PD3-128136233	LDP ECMP topologies no longer cause an error message to be logged when label switched paths (LSPs) are released.
PD3-109003470	The traffic rate no longer drops over a VPLS pseudo wire after an MSM failover and the traffic rate no longer flaps.
PD3-127944432	Configuring a VPLS pseudo wire ID of 0 is not allowed.
PD3-121230737	Extra blackhole entries are no longer added to the FDB for no reason when using VPLS MAC limiting.
PD3-118893434	L2VPN.fecSendFail log messages are no longer generated when disabling MPLS with a large number of VPLSs.
PD3-115971486	Disabling MPLS no longer causes MPLS HAL log messages that may indicate a more serious problem that may require a reboot to correct.
PD3-115548009	A VPLS can be configured to use only a specific named LSP. If the VPLS is UP when the configuration is changed to use a named LSP, but the named LSP is DOWN, VPLS now goes down.
PD3-130672063, PD3-128184768	Changing the Ethernet type on a VPLS service vMAN no longer causes the device to stop forwarding traffic.
PD3-99484115	When disabling MPLS with a large number of VPLSs, the VC labels associated with a VPLS session are no longer removed, which was resulting in the wrong labels being programmed into the hardware.
PD3-125485371	When numerous RSVP-TE LSPs are configured, enabling and quickly disabling RSVP-TE no longer causes data corruption, resulting in a system crash.
PD3-124219816	Disabling and enabling MPLS no longer causes LDP sessions to stay in a non-existent state.
PD3-121206111	VPLS no longer writes a value of 0 to configuration files for unlimited learning, which was resulting in addresses being blackholed.
PD3-106670928	A timing problem no longer exists that can result in a router not being able to forward multicast traffic to its VPLS peers. This problem was triggered by rebooting, disabling and then enabling MPLS, or disabling and then enabling VPLS.

Table 35: General and Platform-Specific Resolved Issues (Continued)

PD Number	Description
PD3-112398430	Globally enabling IP forwarding on all VLANs no longer results in IP forwarding being enabled on VPLS service VLANs.
PD3-115936761	If LDP is not configured to advertise RIP routes, and the configuration is changed such that LDP should advertise RIP routes, the actual RIP route advertisement is now shown.
Multicast	
PD3-73130391	The `unconfigure pim` command no longer removes an SSM configuration while leaving the SM configuration unchanged.
PD3-101466421	IGMP group membership times out after 260 seconds (host time out) if no further IGMP report is received.
Network Services	
PD3-94878540, PD3-78350716	ARP refresh is now working properly when the ARP refresh timeout value is set to two minutes. The ARP entry is reset back to 0, and the timer starts again.
PD3-74503208	The switch does not reject MLD report messages even if the IPv6 destination address is not the same as in the ICMPv6 group field.
PD3-127693933	With a vMAN ethertype configured as 0x8100, and the MAC-in-MAC vMAN is configured with EAPS, dynamic load sharing with LACP is now working correctly and LACP is receiving PDUs from the other end.
PD3-74553139	An MLD packet with a hop-limit of two or more in the IPv6 header is now rejected by the MLD module.
PD3-99950334	UPM profiles no longer fail to load due to a line ending with the > operand.
PD3-129544701	A vMAN policy-based link aggregation group now works if a port-based algorithm is used.
PD3-125157636, PD3-77236566	IPv6 configuration changes, such as clear neighbor-discovery cache ipv6, or unconfiguring the IPv6 addresses on a VLAN no longer generate warning messages.
OSPF	
PD3-75244199	OSPF can now be restarted after a failover and before the backup MSM is fully synchronized.
Routing Manager	
PD3-124609842	A route manager task crash no longer occurs within three minutes of disconnecting and reconnecting an IBGP neighbor. This only occurred when the switch was configured to export a default route into BGP.
ScreenPlay	
PD3-123616718	When using the web user interface, the radio buttons in the RADIUS, TACACS, and Global password policy pages are no longer in the enabled or disabled state.
PD3-124132426	The ExtremeXOS ScreenPlay Help feature now points to the correct documents.
PD3-115071929	QoS monitoring has two types of statistics: ingress and egress. ScreenPlay now shows egress statistics.
PD3-118436421	The port-list is no longer showing ports outside the grid display area in Internet Explorer and Microsoft Windows.
PD3-125715730	The values for the power control unit are now populated in the Inventory grid.
PD3-130084646	The `show log` command no longer returns logs messages lesser than the number of log messages in the switch.
PD3-130084878	The input voltage value for the power portion of a Summit X450 series switch no longer displays an invalid value.
PD3-130099713	An error is no longer displayed when a user password is changed.
PD3-123851170	In the sessions grid, when the value for the IP address for the sessions whose type =XML is ";;" the CLI no longer returns the same value. The Auth type for those sessions are now authenticated by TACACS+.

Table 35: General and Platform-Specific Resolved Issues (Continued)

PD Number	Description
Security	
PD3-126683421	DHCP secured ARP entries are now removed when the DHCP snooping entry ages out in a bootprelay setup.
Spanning Tree Protocol	
PD3-76234725	When load sharing is disabled, the STP related configurations on the load shared ports are no longer lost.
PD3-67562861	With multiple alternate ports, removing MSTI root or making MSTI root inferior no longer causes several topology changes.
PD3-75882801	CIST ports no longer remain in the disabled state when MSTP is configured in a specific order.
PD3-13016876	Traffic is no longer dropped when receiving inferior BPDUs.
PD3-92702567, PD3-105062392	When a port becomes an alternate port, the switch now sends out an alternate proposal for that port.
Stacking	
PD3-129682911	When stacking is enabled, the front panel port LEDs now light for all slots.
VRRP	
PD3-95580434	VRRP configurations on two neighboring and connected switches no longer experience state changes.
PD3-95938607	Configuring an advertised interval at 100 milliseconds with more than 64 VRRP instances no longer causes dual masters on the BlackDiamond 8800 series, BlackDiamond 10808, and BlackDiamond 12804 switches.
PD3-124073369	Creating 128 VLAN-based VRRP instances with eight tracked IP routes for each VRRP instance no longer results in all 128 VRRP instances getting stuck in the INIT state.
WAN PHY	
PD3-100172621	WAN PHY overhead values are no longer displayed twice at the bottom of the WAN PHY Port Overhead screen if Enter is pressed multiple times.